D. G. SWEIGERT, PRO SE, C/O,
MAILBOX, PMB 13339
514 Americas Way, Box Elder, SD 57719
Spoliation-notice@mailbox.org

January 19, 2023

CASE #: 4:22-cv-12696-SDK-APP

District Judge Shalina D. Kumar
U.S. District Court
Eastern District of Michigan
231 W. Lafayette Blvd.
Detroit, MI 48226

SUBJ: Supplement to pre-motion letter requesting an additional 30 days to serve defendants pursuant to F.R.C.P. Rule 4(m).

Your Honor,

1. This letter seeks to supplement ECF doc. 4.

2. Jason Goodman, the sole stockholder of Defendant Multimedia Systems Design, Inc., has named the undersigned as a defendant the Southern District of New York (see attached).

3. The following paragraphs are duplicative of the initial complaint (ECF no. 1) and demonstrate an overlapping relationship between the two lawsuits.

a. Para. 28, page 6 of 127
b. Para. VI. (b), 23 of 127
c. Para. VI. (d), 25 of 127
d. Para. 53, page 35 of 127
e. Para 81, page 41 of 127

4. The undersigned provides a certification that the attached exhibit is a true and accurate representation of the document as published by Mr. Goodman, sole stockholder of Defendant M.S.D.I.

Signed this 19th day of January 2023.

Hereby certified that a PDF copy of this letter has been sent via electronic mail to:

Jason Goodman, sole stockholder of MULTIMEDIA SYSTEM DESIGN, INC.

truth@crowdsourcethetruth.org

Certified under penalties of perjury.

Signed this 19th day of January 2023.

PRO SE
D. G. SWEIGERT, C/O
MAILBOX, PMB 13339
514 Americas Way, Box Elder, SD 57719
Spoliation-notice@mailbox.org

IN THE UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF NEW YORK

JASON GOODMAN Plaintiff, vs. CHRISTOPHER ELLIS BOUZY, BOT SENTINEL, INC, GEORGE WEBB SWEIGERT, DAVID GEORGE SWEIGERT, BENJAMIN WITTES, NINA JANKOWICZ, ADAM SHARP, MARGARET ESQUENET, THE ACADEMY OF TELEVISION ARTS AND SCIENCES, SETH BERLIN, MAXWELL MISHKIN Defendants	Case No.: 1:21-cv-10878-AT-JLC **AMENDED COMPLAINT FOR FRAUD, DEFAMATION, ABUSE OF PROCESS, CIVIL CONSPIRACY, AND RACKETEERING** **JURY TRIAL DEMANDED**

Pro Se plaintiff Jason Goodman ("Goodman") alleges as follows, upon actual knowledge with respect to himself and his own acts, and upon information and belief as to all other matters.

NATURE OF THE ACTION

1. This is an action alleging fraud, defamation, conspiracy to commit fraud, conspiracy to defame, abuse of process, and racketeering, all arising from a scheme between Defendants that was calculated and implemented to financially damage Plaintiff, destroy his news broadcasting business, destroy his valuable branded social media accounts, deprive him of income and prevent him from reporting well founded claims that allege criminal activity on the part of the Defendants and others.
2. Defendants worked together toward a common purpose by filing mass complaints with social media providers using inauthentic accounts, making false claims, and

fraudulent misrepresentations intended to forcibly terminate Goodman's video broadcasting business, and to extort money from him through vexatious litigation including multiple simultaneous lawsuits based on frivolous and fraudulent claims.

3. Defendants engaged in a pattern of racketeering activity including the formation of an association-in-fact enterprise (the "Enterprise") for the purpose of harassing Plaintiff, destroying his business and public reputation, and preventing him from broadcasting findings of his investigations by wrongfully terminating his access to social media.
4. Defendants worked toward a common purpose, with a common goal and continuity for more than five years, up to today, violating 18 U.S. Code § 1962(a)(b)(c) and (d).
5. Defendants' pattern of related racketeering activities caused proximate financial damage to Goodman beginning in 2020, continuously up to and including today.
6. Defendants abused regularly issued civil process with the intent to harm Goodman without excuse or justification and used regularly issued civil process in a perverted manner to achieve the collateral objective of financially destroying Goodman.
7. Defendants repeatedly published known false statements to third parties without privilege or authorization and with the sole intent of defaming and harming Plaintiff.
8. Defendants worked together, sharing information between one another and additional non-parties over the internet, telephones and by other means, amplifying each other's messages on social media, and inappropriately assisting one another across a range of vexatious legal actions filed in numerous divisions of multiple U.S. District Courts.

9. Defendants conspired to damage Goodman's business and reputation by exposing him to public hatred, contempt, and aversion, and by inducing an unsavory opinion in the minds of social media users and the general public with known false statements.

10. Defendants' defamatory statements are inherently harmful to Goodman's reputation due to the heinous nature of the fabricated allegations which included terrorism, rape, and other capital crimes. Such false claims rise to the level of defamation per se and damages to Goodman's reputation and business are presumed.

11. Defendants conspired to commit fraud on the court in their ongoing effort to overwhelm Goodman with abusive litigation and financially crippling legal expenses.

12. Goodman seeks to find all Defendants jointly and severally liable to the extent of,

    a. treble the damages incurred due to Defendants' unlawful activity including attorneys' fees and costs associated with defending Goodman's dormant corporation pursuant to Federal RICO statutes,

    b. costs and expenses spent bringing and defending this and other lawsuits caused by Defendants and,

    c. $2,200,000 in lost business revenue and,

    d. $20,000,000 or an amount otherwise to be decided by a jury in the form of punitive damages for Defendants' illegal, fraudulent and defamatory actions.

PARTIES AND NON-PARTIES

13. Plaintiff – pro se Jason Goodman is a New York citizen, an investigative journalist, documentary filmmaker, talk show host, and founder of the widely trusted news, information, and entertainment brand Crowdsource the Truth. He is separately the

owner of Multimedia System Design, Inc., ("MSD") a dormant New York corporation with no employees, no regular revenue, and no ongoing business activity.

14. Defendant – Christopher Ellis Bouzy ("Bouzy") is a New Jersey citizen and CEO of Bot Sentinel, Inc., which claims to be an artificial intelligence technology company that identifies and eliminates so called "disinformation" as determined by Bouzy.

15. Defendant – Bot Sentinel, Inc., ("Bot Sentinel") is a New Jersey Corporation that claims to be an online platform intended to detect and eliminate untrustworthy internet activity using artificial intelligence and machine learning among other things.

16. Defendant – David George Sweigert ("Sweigert") is believed to be a homeless vagrant, a retired Air Force radio communications and Information Technology specialist, a professional hacker, the author of the Ethical Hacker's Field Operations Guide, a self-proclaimed contractor to the U.S. Department of Homeland Security and other government agencies, and an aggressive, persistent, vexatious pro se litigant. Sweigert is the author of the online blog www.sdny.org which purports to engage in "Disinformation Governance in the Southern District of New York" but is actually a platform for amplifying false claims against Goodman. **(EXHIBIT A)**

17. Defendant – George Webb Sweigert ("Webb") is a homeless vagrant who currently claims to be a citizen of Georgia and a journalist. Webb and Sweigert are brothers (collectively hereinafter "Sweigerts" or "Sweigert Brothers").

18. Defendant Benjamin Wittes ("Wittes") is a self-proclaimed legal journalist, a Senior Fellow in Governance Studies at the non-profit think tank the Brookings Institution and the Editor in Chief of the website Lawfareblog.com ("Lawfareblog").

19. Defendant Nina Jankowicz (“Jankowicz”) is the sole proprietor of Sophias Strategies, LLC, (“Sophias Strategies”) the former Director of the U.S. Department of Homeland Security Disinformation Governance Board (“Disinfo Board”), and a self-proclaimed expert in so called “disinformation” and Russian internet activity including hacking and internet “bot” deployment.
20. Defendant - Adam Sharp ("Sharp") is the founder and CEO of Sharp Things, LLC, the President and CEO of the National Academy of Television Arts and Sciences, (“NATAS”) the former Government Liaison for Twitter, a widely recognized social media expert, and self-proclaimed “Democrat Political Operative”.
21. Defendant – Margaret Esquenet ("Esquenet") is an attorney with Finnegan, Henderson, Farabow, Garrett & Dunner, LLP (“Finnegan”) who represented Defendants in prior action against Goodman’s dormant corporation MSD.
22. Defendant – The Academy of Television Arts and Sciences ("ATAS" or “Television Academy”) is one of the key plaintiffs in a vexatious suit wrongfully brought against Goodman’s dormant corporation MSD for an improper purpose.
23. Defendant – Seth Berlin ("Berlin") is an attorney with Ballard Spahr and counsel for Bouzy and Bot Sentinel in this case.
24. Defendant – Maxwell Mishkin ("Miskin") is an attorney with Ballard Spahr and counsel for Bouzy and Bot Sentinel in this case.
25. Non-Party – Robert David Steele (“RDS”) is a self-proclaimed retired Central Intelligence Agency (“CIA”), employee and the former director of the non-profit

corporation Earth Intelligence Network ("EIN"). RDS was an associate of Webb who reportedly died of Covid-19 in 2021.

26. Non-Party – Kathy Steele ("Steele") is the wife of RDS and executor of his estate. Steele replaced RDS as plaintiff in ongoing litigation against Goodman during 2021. (*See* Steele et al v Goodman Case 3:21-cv-00573-JAG).

27. Non-Party – Steven Biss ("Biss") is the attorney for Steele and formerly RDS. Biss is an associate of Sweigert and communicates with Sweigert through intermediaries.

28. Non-party Richard Loury ("Loury") is a clerk at the U.S. District Court in the Eastern District of Michigan ("MIED").

29. Non-Party – Charles Ortel ("Ortel") is a close and trusted associate of Goodman who is innocent of any wrongdoing in this matter and may have been the initial target of suspected criminal activities of the Enterprise.

30. Non-Party – Peter W. Smith ("Smith") is a deceased former commodities investor, political activist, researcher, and former associate of Ortel.

31. Non-Party – Shane Harris ("Harris") is a journalist and associate of Wittes who wrote several news stories about Smith beginning approximately six weeks after his death. Harris coincidentally contacted Ortel by telephone unexpectedly during Ortel's initial meeting with Goodman and Webb on June 30, 2017.

32. Non-party – Oakey Marshall Richards ("Richards") is an associate of Webb, a confidential informant ("CI") for the Federal Bureau of Investigation ("FBI") and journalist's source of information to Webb regarding events in the Port of Charleston, SC on June 14, 2017, and other matters.

33. Non-party – Roy Warren Marshall aka Steve Quest ("Marshall") is a notorious internet personality (alternately known as "Montagraph"). Marshall is infamous for antagonizing and harassing people online and fixating on toxic vendettas calculated to include real world consequences. Marshall posted videos on YouTube in the days prior to the June 14, 2017 Port of Charleston closure that are likely to prove he and other individuals had prior knowledge of a pre-planned event.

34. Non-party – Scott Anthony ("Anthony") is a New Jersey Information Technology specialist and an associate of Marshall and Sweigert. Anthony posted comments on his web page and in response to videos posted by Marshall on YouTube in the days prior to the June 14, 2017 Port of Charleston closure that are likely to prove Anthony and other individuals had prior knowledge of a pre-planned event. **(EXHIBIT B)**

35. Non-party – Jonathan Snyder ("Snyder") is an attorney who formerly represented MSD in litigation with Defendants but withdrew citing harassment by Sweigert.

JURISDICTION AND VENUE

36. This Court has original subject-matter jurisdiction pursuant to 18 U.S.C. § 1964(c) and 28 U.S.C. § 1331 because this action arises under the Federal Racketeer Influenced and Corrupt Organizations Act ("RICO").

37. This Court also has subject matter jurisdiction pursuant to 28 U.S.C. § 1332 because the amount in controversy exceeds $75,000, exclusive of interest and costs and there is complete diversity of citizenship between Plaintiff and the Defendants.

38. This Court has jurisdiction over Plaintiff's related state and common law claims pursuant to the doctrine of supplemental jurisdiction, 28 U.S.C. § 1367.

39. This Court has personal jurisdiction over Defendants under 18 U.S.C. § 1965(b) because pursuant to the RICO statute, an action brought in any U.S. District Court allows that Court to summon parties residing in another district to its own if the "ends of justice require" as is the case in this instant matter.

40. This Court has personal jurisdiction over Defendants because they deliberately directed their conduct at this forum, at Goodman in New York, and at the Court itself.

41. This Court has personal jurisdiction over Bouzy because he directed conduct at this forum when he participated in the Enterprise. The exercise of jurisdiction over Bouzy is reasonable because he conspired with Defendants to destroy Goodman's business and reputation and terminate his access to social media using Bot Sentinel technology under his own control with the objective of harming Goodman. This Court has personal jurisdiction over Bouzy because he participated in a scheme in violation of 18 U.S. Code § 1513 to retaliate against Goodman for bringing legal action against him and Bot Sentinel. This Court also has personal jurisdiction over Bouzy under 18 U.S. Code § 1965(b) which allows any District Court to summon parties from another district if the "ends of justice require" it.

42. This Court has personal jurisdiction over Bot Sentinel because it directed conduct at this forum when it participated in the Enterprise. Exercise of jurisdiction over Bot Sentinel is reasonable because it conspired with Defendants to destroy Goodman's business and reputation and terminate his access to social media using Bot Sentinel technology under Bouzy's control with the objective of harming Goodman. This Court also has personal jurisdiction over Bot Sentinel because it participated in a

scheme in violation of 18 U.S. Code § 1513 to retaliate against Goodman for bringing legal action against it and Bouzy. This Court also has personal jurisdiction over Bot Sentinel under 18 U.S.C. § 1965(b) which allows any District Court to summon parties from another district if the "ends of justice require" it.

43. This Court has personal jurisdiction over Sweigert because he directed conduct at this forum when he participated in the Enterprise. The exercise of jurisdiction over Sweigert is reasonable because he conspired with Defendants to destroy Goodman's business and reputation and terminate his access to social media by conspiring with Bouzy to use Bot Sentinel technology under Bouzy's control with the objective of harming Goodman. This Court also has personal jurisdiction over Sweigert because he participated in a scheme in violation of 18 U.S. Code § 1513 to retaliate against Goodman for filing an Amicus Curiae brief in support of Cable News Network ("CNN") by ghost writing vexatious pleadings on behalf of Webb in violation of NYCL - EDN § 6512. This Court also has personal jurisdiction over Sweigert under 18 U.S.C. § 1965(b) which allows any District Court to summon parties from another district if the "ends of justice require" it.

44. This Court has personal jurisdiction over Webb because he directed conduct at this forum when he participated in the Enterprise. The exercise of jurisdiction over Webb is reasonable because he conspired with Defendants to destroy Goodman's business and reputation and terminate his access to social media with the objective of harming Goodman. This Court also has personal jurisdiction over Webb because he participated in a scheme in violation of 18 U.S. Code § 1513 to retaliate against

Goodman for filing an Amicus Curiae brief in support of CNN by filing a frivolous retaliatory case against Goodman. This Court also has personal jurisdiction over Webb under 18 U.S.C. § 1965(b) which allows any District Court to summon parties from another district if the "ends of justice require" it.

45. This Court has personal jurisdiction over Wittes because he directed conduct at this forum when he participated in the Enterprise. The exercise of jurisdiction over Wittes is reasonable because Wittes conspired with Defendants to destroy Goodman's business and reputation and terminate his access to social media by directing Bouzy to use Bot Sentinel technology under Bouzy's control with the objective of harming Goodman. This Court also has personal jurisdiction over Wittes because he participated in a scheme in violation of 18 U.S. Code § 1513 to retaliate against Goodman for bringing legal action against Bouzy and Bot Sentinel by retaining Ballard Spahr and funding the Enterprise's legal defense. This Court has personal jurisdiction over Wittes under 18 U.S.C. § 1965(b) which allows any District Court to summon parties from another district if the "ends of justice require" it.

46. This Court has personal jurisdiction over Jankowicz because she directed conduct at this forum when she participated in the Enterprise. The exercise of jurisdiction over Jankowicz is reasonable because she conspired with Defendants to destroy Plaintiff's business and reputation and terminate his access to social media by making false claims in violation of 22 U.S. Code § 612 with the objective of harming Goodman. This Court has personal jurisdiction over Jankowicz under 18 U.S.C. § 1965(b) which

allows any District Court to summon parties from another district if the "ends of justice require" it.

47. This Court has personal jurisdiction over Sharp because he directed conduct at this forum when he participated in the Enterprise. The exercise of jurisdiction over Sharp is reasonable because he conspired with Defendants to destroy Goodman's business and reputation and terminate his access to social media by wrongfully bringing action against Goodman's dormant corporation MSD, with the objective of deliberately harming Goodman. This Court also has personal jurisdiction over Sharp because he wrongfully caused tax-exempt funds to be used in violation of New York Not-For-Profit Corporation Law - NPC § 712-a and failed to disclose his interest in a private, for-profit business while employed as CEO of a tax-exempt corporation. This Court also has personal jurisdiction over Sharp because he participated in a scheme to commit fraud on the Court in violation of 18 U.S. Code § 1343 by falsely claiming his private, for-profit corporation Sharp Things, LLC was inactive. This Court has personal jurisdiction over Sharp under 18 U.S.C. § 1965(b) which allows any District Court to summon parties from another district if the "ends of justice require" it.

48. This Court has personal jurisdiction over Esquenet because she directed conduct at this forum when she participated in the Enterprise. The exercise of jurisdiction over Esquenet is reasonable because she conspired with Defendants to destroy Goodman's business and reputation and terminate his access to social media by participating in a scheme to wrongfully bring action against MSD, with the objective of deliberately harming Goodman. This Court also has personal jurisdiction over Esquenet because

she wrongfully accepted tax-exempt funds used in violation of New York Not-For-Profit Corporation Law - NPC § 712-a. This Court also has personal jurisdiction over Esquenet because she participated in a scheme to commit fraud on the Court in violation of 18 U.S. Code § 1343 and New York Judiciary Law - JUD § 487 with the express intent of harming Goodman by falsely claiming Sharp's private, for-profit corporation Sharp Things was inactive. This Court has personal jurisdiction over Esquenet under 18 U.S.C. § 1965(b) which allows any District Court to summon parties from another district if the "ends of justice require" it.

49. This Court has personal jurisdiction over ATAS because it directed conduct at this forum when it participated in the Enterprise. The exercise of jurisdiction over ATAS is reasonable because it conspired with Defendants to financially damage Goodman by wrongfully bringing action against Goodman's dormant New York corporation MSD, with the objective of harming Goodman. This Court also has personal jurisdiction over ATAS because it violated its own by-laws and authorized tax-exempt purpose by wrongfully causing tax-exempt funds to be used in violation of New York Not-For-Profit Corporation Law - NPC § 712-a. This Court also has personal jurisdiction over ATAS under 18 U.S.C. § 1965(b) which allows any District Court to summon parties from another district if the "ends of justice require" it.

50. This Court has personal jurisdiction over Berlin because he directed conduct at this forum when he participated in the Enterprise. The exercise of jurisdiction over Berlin is reasonable because he conspired with Defendants to intimidate Goodman with harassing extrajudicial letters after he was alerted by a Tweet sent by Sweigert and

prior to appearing as counsel for Defendants Bouzy and Bot Sentinel in violation of 18 U.S. Code § 1503.

51. This Court has personal jurisdiction over Mishkin because he directed conduct at this forum when he participated in the Enterprise. The exercise of jurisdiction over Mishkin is reasonable because he conspired with Defendants to intimidate Goodman with harassing extrajudicial letters after he was alerted by a Tweet sent by Sweigert and prior to appearing as counsel for Defendants Bouzy and Bot Sentinel in violation of 18 U.S. Code § 1503.

FACTUAL BACKGROUND

18 U.S.C. § 1962 makes it unlawful for any person to receive any income derived, directly or indirectly, from a pattern of racketeering activity. Defendants in this case have engaged in a wide-ranging pattern of racketeering activity that began in 2017 and began causing direct and proximate financial damage to Goodman in 2020, continuously up to and including today. Defendants attempt, in an ongoing fashion, to conceal their efforts using sophisticated technology including encrypted and clandestine messaging techniques. Defendants employ deceptive legal tactics designed to manipulate and hinder both civil and criminal justice processes and hide their individual culpability and their direct or indirect coordination. Despite strenuous efforts to conceal these alleged acts, evidence presented herein is likely to prove that Defendants formed and actively participated in the Enterprise with common objectives that included the destruction of Goodman's business and public reputation, extortion of money from him via vexatious and fraudulent litigation, and the total elimination of his access to social media. The Enterprise operates as a dynamic online collective which Sweigert himself refers to

as a ("Cyber Militia"). The Cyber Militia enables coordinated activity through deceptive anonymous online accounts and a multitude of clandestine, encrypted communication schemes to amplify each other's efforts and create public perception of an authentic grass roots movement that disfavors Goodman, his investigative reporting, and his video subscription business.

I. Multimedia System Design, Jason Goodman, and Crowdsource the Truth

Goodman is the sole proprietor of MSD, a corporation he founded in 1994 originally focused on computer network design and maintenance for graphic arts and multimedia professionals. As years passed, the focus of the company shifted toward the creation of 3D animation and multimedia software-based business presentations rather than computer hardware services. In May of 1998, Goodman applied for and received the assumed name "Multimedia Software Design" to better reflect the evolving nature of the business. Years later, the company focused even more closely on 3D animation and stereoscopic video production. Goodman again applied for an assumed name with the New York Department of State and established "21st Century 3D". **(EXHIBIT C)**

Goodman had a lucrative career in Hollywood for many years where he became internationally recognized as one of the world's foremost experts in stereoscopic cinematography and 3D camera design and development. Multimedia System Design, INC., D.B.A. 21st Century 3D operated offices in New York and Los Angeles. In or around 2013, 3D moviegoing and production crashed and virtually all of Hollywood's 3D providers including 21st Century 3D ceased operation. Goodman returned to New York in or around 2015 and worked to re-establish himself in a market that no longer demanded stereoscopic cinematographers. MSD remained active and in good standing but Goodman's role as CEO focused on rare, occasional, specialized

3D work and eventually turned to selling the company's large inventory of valuable professional camera equipment. At the same time, Goodman engaged in the separate unrelated endeavor of creating news, information and entertainment videos using inexpensive mobile phones owned by Goodman on a YouTube channel called "Jason Goodman" with shows bearing the brand name "Crowdsource the Truth" and unrelated to MSD. Leveraging his experience as a producer and cinematographer, and emerging skills as a journalist and talk show host, Goodman built an audience on YouTube and eventually monetized the effort by creating a subscription video service through which individual viewers become monthly sponsors and gain access to sponsor exclusive content on www.patereon.com ("Patreon"), www.subscribestar.com ("SubscribeStar") and www.odysee.com ("Odysee"). MSD is not associated with these platforms or their payment services. Goodman is the sole and exclusive owner of intellectual property and artistic works created by Goodman under the brand name Crowdsource the Truth.

II. The Cyber Militia

For many years, Sweigert has written white papers and blog posts and conducted online video seminars about his perceived need for a Digital National Guard to protect the country against cybersecurity threats to critical U.S. Infrastructure. **(EXHIBIT D)**

Sweigert's proposed civilian staffed Cyber–National Guard unit could be stood up on demand to act defensively or offensively according to Sweigert. He uses the phrase "Cyber Militia" as he addresses his online pupils stating in part, "I'm working around waiting for consensus from government people or industry people or people like that. We're moving ahead with the actual scenario that's going to be used by actual infrastructure operators. I guarantee you what we're doing right now is going to be documented and it's going to be read by several dozen

key people That run the critical infrastructure of the United States."

(https://vk.com/video731682021_456239025)

Sweigert has posted numerous videos that he disseminates to members of his Cyber Militia using coded hashtags and other clandestine communication techniques. Like the 1960s television series Misson: Impossible, Sweigert's video messages self-destruct, or rather he voluntarily spoliates them quickly making it difficult to track this activity or provide evidence to the Court. Goodman has successfully archived some of these videos, despite repeated efforts by Sweigert to threaten the video hosting web sites used to preserve the evidence. Several of the videos have been preserved on a website hosted outside the U.S. which Sweigert has been unable to threaten with litigation, allowing the Court to evaluate his activities related to the education, coordination, and deployment of his online cyberstalking gang masquerading as a makeshift military adjunct in his ongoing efforts to accuse Goodman of crimes he has not committed and otherwise harass and antagonize Goodman.

(https://vk.com/video731682021_456239067)

(https://vk.com/video731682021_456239073)

III. The Sweigert Brothers and the Port of Charleston Incident

Goodman first interacted with the Sweigert Brothers' Cyber Militia without his knowledge when he began collaborating with Webb in or around May of 2017. Goodman and Webb collaborated for a period of approximately three months, voluntarily cooperating to create video news reports primarily on YouTube. On June 13, 2017, Webb introduced Goodman telephonically to RDS who claimed, without evidence, to be a former employee of the CIA. The three engaged in a video conference interview that was broadcast live on Goodman's YouTube

channel but has since been removed by YouTube as a proximate result of multiple fraudulent complaints filed by Sweigert and his co-conspirators.

Goodman alleges Defendants used tactics including "mass reporting" from a large number of inauthentic accounts to create the false impression of public outrage and prompt the removal of numerous videos and ultimately Goodman's entire YouTube channel while hiding evidence of their actions. Plaintiff has preserved the RDS interview and re-uploaded it to an alternate video host. No similar complaints have forced the removal of the same video from other platforms. (https://odysee.com/@Crowdsourcethetruth:d/Robert-David-Steele:3?r=73LTQ7izBcj8qkyQcMRLcevmePnUuBoJ and https://rumble.com/vm2gg7-robert-david-steele-on-crowdsource-the-truth-june-13-2017.html). Shortly after the initial June 2017 video conference and events resulting inter alia in the arrest of Webb and the closure of the Port of Charleston in South Carolina, RDS brought legal action against Goodman, (*See* Steele et al v Goodman et al, Case 3:17-cv-00601-MHL) alleging defamation and other claims. The case was dismissed without prejudice by Judge M. Hannah Lauck on September 25, 2020 (*See* Steele et al v Goodman et al Case 3:17-cv-00601-MHL ECF No. 217). In defiance of Judge Lauck's order, RDS brought his claims back in the Eastern District of Virginia Alexandria Division (*See* Case 1:20-cv-01140-RDA-IDD Document 12). The case was transferred back to the Richmond Division. RDS is now reportedly deceased, (https://nypost.com/2021/08/30/ex-cia-spy-first-to-call-covid-a-hoax-dies-from-the-virus/) but his estate remains represented in the case against Goodman. A motion for contempt against the substituted Plaintiff and attorney Biss is pending, (*See* Steele v Goodman Case 3:21-cv-00573-JAG ECF No. 39). Sweigert has attempted to

intervene in both iterations of Steele v Goodman but has been denied (*See* Case 3:17-cv-00601-MHL Document 152 and Case 1:20-cv-01140-RDA-IDD ECF No. 8).

In or around June 2022, Goodman discovered a video published by Marshall on June 11, 2017, three days prior to the events related to the Port of Charleston closure. In the video, Marshall includes images of a sinking cargo ship along with the message "George Webb & Jason Goodman are inches away from being superstars for all the wrong reasons". The video also features a message to "Hollywood Executives Worldwide" alerting them to false claims made by Marshall (https://youtu.be/KysTO2GoRB0). This remarkable coincidence is highly suggestive that Marshall and others had foreknowledge of the events that would take place only three days later in the Port of Charleston, for which Goodman would be blamed by Sweigert and RDS. Notably, in a separate video posted by Sweigert in approximately the same timeframe, Sweigert addresses Goodman, making a point of his intention to "call all your Hollywood friends and I'll talk to them and say hey we're gonna make a lot of money on this" perhaps foretelling Sweigert's future communication with Sharp. (https://vk.com/video731682021_456239066).

IV. The Suspicious Death of Peter W. Smith

During Goodman's brief collaboration with Webb, Webb arranged a meeting with Ortel who Goodman had not previously known. During that meeting, Ortel received a phone call about the suspicious suicide of his colleague Smith who had died six weeks prior. The caller, Harris, was a Wall Street Journal reporter at the time and unknown to Ortel. Harris rudely inquired about details allegedly related to a story he would publish about the death of Smith. https://www.wsj.com/articles/gop-operative-sought-clinton-emails-from-hackers-implied-a-connection-to-flynn-1498770851). Due to the suspicious circumstances surrounding Smith's

death, and the curiously coincidental way the information came about, Goodman became intrigued by the incident and began investigating further. Goodman traveled to the Rochester, MN hotel where Smith died. Police crime scene photos revealed two tanks of helium gas that were determined to be the cause of self-inflicted asphyxiation. On that trip, Goodman gathered evidence, including video surveillance footage of Smith purchasing only one helium tank at a nearby Walmart. Interviews with hotel employees and others, provided Goodman with what the Rochester Police described as more evidence than they had prior to closing the case. Goodman's suspicions prompted him to contact Wittes via Twitter because he had hosted Harris on several Lawfareblog podcasts and seemed to be covering the story closely. The term "lawfare" generally refers to the weaponization of legal process and is suggestive of Wittes preferred modus operandi. Wittes did not respond to Goodman's numerous inquiries related to the large amount of evidence Goodman had obtained which contradicted major portions of Harris' and Wittes' reporting. After nearly three years of ignoring Goodman, on or around December 19, 2020, Wittes agreed to engage in a text interview with Goodman over Twitter. Although Wittes agreed to participate voluntarily, he avoided answering pertinent questions and prematurely terminated the session directly coincident with the unexpected interruption of unwanted, disruptive, and insulting public Twitter messages from Bouzy.

V. Twitter, Christopher Bouzy, and Bot Sentinel

Recent events have brought new scrutiny to inauthentic social media accounts known as "bots". Billionaire investor Elon Musk purchased Twitter in 2022 based on his stated goal to eliminate the large number of inauthentic accounts and protect the first amendment rights of Twitter users. (https://finance.yahoo.com/news/musk-calls-twitter-explanation-bot-

071116182.html). Inauthentic so-called "bot" accounts call into question the true value of Twitter as a company and may implicate its board of directors or other former employees including Sharp in Federal Trade Commission and Securities and Exchange Commission violations. Bot Sentinel claims to be a benevolent tool that is free to use and financially supported by donations from magnanimous donors. The truth is, Bot Sentinel is a tool deployed by Bouzy to engage in cyber harassment for hire intended to thwart anyone he opposes and a vehicle through which he can receive anonymous payments. Bouzy frequently boasts of his special relationship with Twitter insiders. Bouzy is a social media hit man who uses Bot Sentinel to target, defame, and destroy the accounts and public reputations of his perceived enemies. Goodman alleges Wittes engaged Bouzy's services to harass Goodman and eliminate his access to social media including Twitter and others, after Goodman published information that was unfavorable to Wittes concerning the death of Smith. Goodman's initial contact with Bouzy came during the Twitter conversation with Wittes. Bouzy's effort to disrupt the Wittes conversation consisted of false claims so offensive and insulting, they prompted Goodman to search the internet for Bouzy's phone number, call him up and speak for more than one hour, (https://odysee.com/@Crowdsourcethetruth:d/BOUZYBOTSENTINEL:a?r=73LTQ7izBcj8qkyQcMRLcevmePnUuBoJ). During the call, Bouzy revealed his direct knowledge of Smith's death and his personal familiarity with Wittes, Harris, and other associates of Lawfareblog. After the phone call, Bouzy began a days-long Twitter defamation campaign against Goodman that included false, baseless, and unsubstantiated claims alleging Goodman had committed the crime of rape. These heinous allegations are inherently damaging and were made with the sole intention of injuring Goodman's reputation and business. Despite these horrendous actions, and

due to Goodman's demanding schedule, he decided to ignore Bouzy and put the harassment and defamation out of mind. Almost one year later, with no further provocation from Goodman, on December 17, 2021, Bouzy republished the same series of defamatory tweets, giving rise to this instant action. Despite explicit warnings from Goodman in 2020, Bouzy chose to join the Enterprise established by the Sweigert Brothers. Not satisfied with mere reputation destruction, Bouzy took further steps to destroy the social media accounts that he knew were critical to Plaintiff's daily business operations. Bouzy received information from Sweigert that he amplified in his efforts to defame and harass Goodman while destroying his business and his access to social media in violation of 18 U.S. Code § 1513.

VI. Years Long Lawfare Assault Against Goodman

a. Steele et al v Goodman et al

Beginning in September of 2017, the Defendants and other non-parties participated in a series of vexatious and abusive lawsuits calculated to harm Goodman. These suits did not seek to cure any legitimate injury but rather to extort Goodman into terminating video broadcasts including evidence from his investigations that is likely to implicate Defendants in criminal activity. The first such suit was Steele et al v Goodman et al (*See* Case 3:17-cv-00601-MHL). Sweigert attempted and failed to intervene in this case and shortly thereafter, brought separate action citing the same Port of Charleston incident and many of the same parties (*See* Sweigert v Goodman Case 1:18-cv-08653-VEC-SDA). Steele v Goodman was incompetently prosecuted by the frequently sanctioned Biss and was dismissed without prejudice in September 2020. Sweigert v Goodman was voluntarily dismissed in March 2022 after more than three years of vexatious litigation. The constantly scheming Sweigert engaged in myriad extrajudicial attacks

during the course of all of the malicious legal action, calculated to complicate Goodman's ability to mount a proper defense while simultaneously disrupting Goodman's daily news broadcasts in the ongoing effort to destroy Goodman's business. Due to Sweigert's ongoing failure to defeat Goodman as a pro se defendant, Goodman alleges Sweigert devised a scheme to financially damage Goodman by making the fraudulent representation that the corporation MSD controlled and was liable for intellectual property owned exclusively by Goodman including images and video content created for Crowdsource the Truth broadcasts, in logical contradiction to 47 U.S. Code § 230. This gave rise to a series of attempts to fraudulently sue Goodman's corporation compelling him to hire counsel at great expense rather than exercising his right to proceed pro se.

b. Sweigert v Goodman (SDNY)

On June 14, 2018, by his own admission in celebration of the one-year anniversary of the Port of Charleston incident, Sweigert commenced new legal action against Goodman in the U.S. District Court for South Carolina. The complaint alleged that Goodman was a cult leader and his news reporting constituted racketeering. (*See* Sweigert v Goodman 2:18-cv-01633-RMG). Sweigert v Goodman was transferred sua sponte pursuant to 8 U.S.C. §§ 1404(a), 1406(a) to the Southern District of New York on September 17, 2018 (*See* Case 1:18-cv-08653-VEC). After more than three years of extensive motion practice, and substantial burden on Goodman, on March 1, 2022, Sweigert voluntarily withdrew his claims, and the case was dismissed with prejudice. (*See* Case 1:18-cv-08653-VEC-SDA ECF No. 381). Sweigert, apparently dissatisfied with this outcome and determined to bring back the same claims in another U.S. District Court where he might further harass Goodman, submitted a motion for reconsideration seeking to grant dismissal without prejudice. The motion was denied. (*See* Sweigert v Goodman Case 1:18-cv-

08653-VEC-SDA Document 383). Despite the dismissal with prejudice, and admonishment by the judge for excessive filing, Sweigert has continued to file in the case. Most recently a completely inappropriate letter was sent to chambers on Christmas eve raising incoherent claims related to Steele et al v Goodman and other matters. (*See* Sweigert v Goodman Case 1:18-cv-08653-VEC-SDA Document 387)

c. Sweigert v CNN

On October 31, 2020, Webb brought action against Cable News Network ("CNN") in the Eastern District of Michigan ("MIED") as a pro se Plaintiff including allegations of defamation and other things. (*See* Webb v CNN Case 2:20-cv-12933-GAD-KGA)**.** Despite their own public claims that the Sweigert Brothers are estranged and not in regular communication, Sweigert filed a motion to intervene in his brother Webb's case less than one week later on November 6, 2020. The motion additionally sought to transfer the case to SDNY claiming it was related litigation and citing the still ongoing at the time Sweigert v Goodman.

Evidence presented to the MIED court is likely to prove that Sweigert fraudulently submitted filings on his brother Webb's behalf, practicing law without a license in the State of Michigan in violation of Michigan Legislature - Section 600.916 and for the express purpose of entangling Goodman in more vexatious litigation. On July 20, 2021, Goodman filed an Amicus Curiae brief in support of defendant CNN's motion to dismiss which presented evidence that is likely to prove that Webb and Sweigert conspired with a clerk of the court, Loury, to cause a fraudulent document to be filed on the docket, in violation of 18 U.S. Code § 1343 attributed to Webb, but authored by Loury, and outside the normal procedure of the MIED Court's Pro Se Electronic Filing website. (*See* Case 2:20-cv-12933-GAD-KGA ECF No. 20)

On September 21, 2021, presiding Judge Gershwin Drain issued a notice of motion hearing set for December 16, 2021. The order was sent by U.S. Postal Service to Goodman, summoning Goodman to the hearing (*See* Case 2:20-cv-12933-GAD-KGA ECF No. 24). On November 1, 2021, an order replacing the in-person motion hearing with a December 20, 2021 Zoom telephonic hearing was issued (*See* Sweigert v CNN Case 2:20-cv-12933-GAD-KGA ECF No. 28). On December 14, 2021, another order was issued rescheduling the motion hearing for an in-person hearing. (*See* Sweigert v CNN Case 2:20-cv-12933-GAD-KGA ECF No. 34). Goodman traveled to MIED as ordered at his own expense. Only hours after arriving, one day before the scheduled hearing, an email was sent by Teressa McGovern from Judge Drain's chambers stating in part, "The Court is adjourning tomorrow's hearing. The Court will reach out at a later date to reschedule this hearing."

The hearing was not adjourned but rather canceled and never rescheduled. On March 14, 2022, Goodman filed a motion seeking leave to file an amended Amicus Curiae brief and included a substantially larger amount of evidence that is likely to prove Webb and Sweigert conspired with Loury to file a fraudulent pleading on the docket (*See* Case 2:20-cv-12933-GAD-KGA ECF No. 55). On March 21, 2022, without oral arguments or examination of Goodman's evidence, Judge Drain issued an order inter alia granting CNN's motion to dismiss, striking Goodman's amicus curiae brief, denying Sweigert's request for change of venue, denying non-party Goodman's motion for leave to file amended amicus curiae brief and dismissing the action. It is noteworthy that Judge Drain mistakenly attributed Sweigert's request for change of venue to plaintiff Webb, providing evidence that the brother's interoperability succeeded in confusing the court.

d. Sweigert v Goodman (MIED)

Concurrent with his case against CNN and ostensibly as retaliation for filing the well-founded accusations in the Amicus Brief, on January 3, 2022, Webb brought action against Goodman in MIED alleging defamation for the privileged statements in the amicus brief. (*See* Sweigert v Goodman Case 2:22-cv-10002-GAD-KGA). Four days later on January 7, 2022, non-party Sweigert began interfering again filed a request for criminal referral against Goodman. Sweigert made a facially ridiculous attempt to deceive the court by miscategorizing Goodman's rightful response to Judge Drain's order that he attend a hearing as an effort to stalk Webb in Michigan. Sweigert goes on to falsely state "Mr. Goodman worked as a camera operator on a Bryan Singer film, X-Men" and adds "There were alleged accusations that orbited the drugging and rape of underaged actors at parties supposedly attended by Mr. Goodman." Goodman has never worked as a camera operator on a Bryan Singer film, has never attended any party where anyone was drugged and raped and has never met Singer. No such allegations exist apart from false allegations promulgated by the Sweigert brothers and their associates including Defendant Bouzy. (*See* Sweigert v Goodman Case 2:22-cv-10002-GAD-KGA). On April 1, 2022, Judge Drain transferred the case to SDNY. After clogging the docket with spurious false allegations, wasting more of Goodman's time and money, and burdening him with additional vexatious litigation, on July 19, 2022, Webb voluntarily withdrew the case in a manner remarkably similar to Sweigert's previous action. (*See* Case 1:22-cv-02788-LGS-BCM ECF No. 73). Evidence on the docket is likely to prove this case was brought by Sweigert in his brother Webb's name, in violation of 18 U.S. Code § 1343, Michigan Legislature - Section 600.916, and NYCL - EDN § 6512. Sweigert had learned from his previous voluntary withdrawal that failure to request

dismissal without prejudice, left the decision to the judge. His choice to seek dismissal without prejudice is strong evidence that Sweigert authored the pleading and filed on Webb's behalf.

VII. The Television Academy and Multimedia System Design, Inc.

By August 2020, the Jason Goodman YouTube channel had grown to amass approximately 119,000 subscribers and had generated tens of millions of video views. This channel provided a large and rapidly growing pool of new potential customers for Goodman's paid video subscription service which is his primary source of income. Unlike many popular YouTube channels, Goodman does not rely on Google advertising revenue to earn a living. This is primarily due to Goodman's objection to corporate sponsorship of news and his opinion that the practice puts interests of paying corporations ahead of individual viewers. In addition to revolutionizing the video production of news programming by utilizing low cost, high-definition video cameras embedding in inexpensive mobile phones and operating as "one man band" to produce sophisticated broadcasts normally associated with network television, Goodman was very early to the market of direct to consumer, rather than corporate sponsored programming. This disruptive business model flies in the face of the traditional approach relied upon by broadcast television and Defendant ATAS and may further their motivation to destroy Goodman.

On June 12, 2020, Goodman produced a video called the "Crony Awards" which featured a thumbnail image including a parody of the Television Academy's well known EMMY statue. Section 107 of the Copyright Act states in part "In the United States, parody is protected by the First Amendment as a form of expression. However, since parodies rely heavily on the original work, parodists rely on the fair use exception to combat claims of copyright infringement." It is widely recognized that copyright creators are likely to disfavor parodies of their work as they are

often the target of the parodist's criticism as is the case here. Goodman believes the television industry and Sharp's academy that supports it have been corrupted by greed and the corporate drive for increasing profits. To this end, Goodman created a program that was intended to mock corporate television news broadcasts and shows that award them for poor coverage of, and contribution to, the widespread panic and societal destruction caused by the Covid pandemic.

Contrary to Defendants' ridiculous claims, Goodman's broadcast of the "Crony Awards" was not an actual awards show. No nominees or guests were invited, no actual awards were given. The broadcast was itself a parody of those events and focused on countries around the world that had remarkably better outcomes in their public health policies toward Covid-19 than the United States. More than two months after the publication of the Crony Awards video, on or around August 20, 2020, the Jason Goodman YouTube channel received a Copyright Complaint resulting in a penalty from YouTube known as a strike. This strike on the YouTube channel is a stain that impacts the channel and a user's access to it in several ways. First and foremost, at that time in 2020, YouTube policy prevented any new broadcasts for a period of ninety days. This was especially troubling given that it threatened to prevent Goodman from broadcasting during the historic and now controversial 2020 Presidential election.

Goodman has suspected from the outset of the dispute that this was the true motivation behind the fraudulent YouTube copyright complaint, filed in violation of 18 U.S. Code § 1343 and the subsequent equally fraudulent lawsuit. Rather than expeditiously curing the perceived injury at no cost, Sharp sought to abuse regularly issued civil process in a perverted manner with the collateral objective of forcibly preventing Goodman from broadcasting during the 2020 election. Beyond the immediate damage of lost revenue and subscriber growth during an

historic, once in a lifetime event, as YouTube strikes accumulate, a total of three strikes permanently deletes the channel and this was the ultimate outcome in this case. The total removal of Goodman from the internet including YouTube has been the stated goal of Sweigert and his Cyber Militia for many years. It is unlikely Sharp would randomly encounter a two-month-old video as initially alleged. Given the specific timing of the complaint relative to the 2020 election and Sweigert's incredibly persistent, near daily pursuit of Goodman, it appeared highly likely that Sweigert concocted a scheme with Sharp to file the complaint with YouTube in August so the ninety-day penalty would preclude Goodman from broadcasting during the election. Even if there were no preconceived plan between Sweigert and Sharp, Defendants' original complaint filed in NATAS v MSD reveals that the alleged "gross" trademark violation was reported via an "anonymous" email on Tuesday July 28, 2020. (*See* Case 1:20-cv-07269 ECF No. 1 page 9 paragraph 33). If the alleged infringement was so offensive, it would logically follow that a YouTube complaint would be issued immediately or within days. No other circumstance can explain the nearly one-month delay in filing the complaint against the Jason Goodman YouTube channel followed by the rush to litigation once Goodman appealed the complaint and restored his ability to broadcast. Under YouTube rules, the initiation of litigation reinstates the penalty after a YouTube appeal has lifted it and resumes blockage of broadcasting, pending resolution of the lawsuit.

Goodman alleges, Sweigert, Sharp, ATAS, and Esquenet conspired to calculate the false copyright infringement claim and subsequent lawsuit for the ulterior purpose of applying a ninety-day penalty and blocking Goodman from broadcasting prior to and during the election on his popular and widely viewed YouTube channel which favored candidate Donald Trump.

This horrendous breach of Bar Association ethics, the rules, the law, and basic morality is beyond the pale. Defendants have gone to extraordinary lengths to prevent Goodman from learning the true identity of the owner of the stipulated confidential email address that was the genesis of their malicious abuse of process against Goodman and his corporation. This is also further evidence that only Sweigert could be responsible for sending the anonymous email that alerted Sharp of the alleged infringement. Sharp declined to respond to emails sent in response to the YouTube complaint. From the outset, Goodman warned Sharp of his serious concern that an outside party was intent on drawing Sharp and the non-profit Television Academy into expensive protracted litigation. Goodman offered several suggestions including the total removal of the offensive image but got no response from Sharp. **(EXHIBIT E)**

Instead of entertaining Goodman's no-cost proposal of deleting the parody image, Sharp immediately retained Finnegan. The firm is one of the largest in the field of intellectual property law and likely expensive to retain. This approach made very little sense to Goodman, particularly for a non-profit that ordinarily would compel executives to operate in its own best financial interest and not rush to litigate the way a for profit private sector company might. Goodman engaged with Esquenet initially by email and soon after by telephone. Goodman reiterated his well-founded belief that Sweigert was deliberately interfering in this matter, had likely alerted Sharp of the parody image and did so with the express intent of drawing Sharp and ATAS into litigation against Goodman, which did happen immediately thereafter as if preordained. Further to Goodman's surprise, his corporation MSD, which had nothing to do with the broadcast or Goodman's intellectual property contained therein and is not even mentioned anywhere on the YouTube channel, was the target of the suit. Goodman alleges this

was a calculated plan, formulated by Sweigert, Sharp, ATAS, and Esquenet to compel Goodman to hire legal counsel to defend his corporation because he had proven too difficult to defeat as a pro se defendant. To wit, there is no conceivable way Sharp or Esquenet could know of Goodman's ownership of MSD if not for being informed by Sweigert. Defendants will fail to prove they learned of the corporation in any other way. This is the essence of their scheme to maliciously sue the unrelated MSD in contradiction to 47 U.S. Code § 230 and violation of 18 U.S. Code § 1343, for the ulterior purpose of forcibly terminating Goodman's popular broadcasts during the 2020 Presidential election because they disagree with him politically.

Throughout the course of National Academy of Television Arts and Sciences v Multimedia System Design, ("NATAS v MSD"), Sweigert continued his vexatious interference, not only trying and failing once again to intervene (*See* Case 1:20-cv-07269-VEC-OTW ECF No. 84) but also aggressively harassing MSD's counsel Snyder. Snyder ultimately withdrew after failing to represent MSD according to Goodman's instructions specifically citing Sweigert's harassment as his reason (*See* Case 1:20-cv-07269-VEC-OTW ECF No. 102-2). Despite this incredibly inappropriate and highly strategic interference, even while simultaneously presiding separately over Sweigert v Goodman (*See* Case 1:18-cv-08653-VEC-SDA), Judge Valerie Caproni took no action whatsoever to curtail Sweigert's grossly inappropriate conduct which violated 18 U.S. Code § 1503 and 18 U.S. Code § 1513. Sweigert interfered further with near daily agitating emails directed at Goodman and the attorneys at Finnegan including Esquenet who Sweigert addressed as his "team".

Esquenet and her associates behaved in ways that confirmed Sweigert's assertion that they operated as a clandestine team despite overt denial of that allegation. During discovery in

the case, Esquenet utilized information received from Sweigert, requesting MSD produce emails sent from the address CSTT72@protonmail.com. This email address is not owned or controlled by Goodman or MSD, but rather is believed to be controlled by a British national named James Bembridge who is an associate of Sweigert, and a member of the Cyber Militia engaged in harassing Goodman. Just as with Goodman's corporation, there is simply no way Defendants could have learned of this email address without the direct or indirect cooperation of Sweigert.

Unable to obtain new counsel after Snyder's astonishing withdrawal, MSD ultimately defaulted in the case which is currently on appeal with the Second Circuit (*See* Cass 22-592). Goodman is in the process of writing a 60(b)(3) motion to be filed with the District Court. In addition to the information presented herein, subsequent to the default judgment, Goodman has learned that in 2009 while serving as the first in history General Counsel of the FBI, Judge Caproni appeared on C-SPAN3 during the time Sharp was Executive Producer and Programming Director. The subject of Judge Caproni's appearance was a problem she described as the FBI "Going Dark". This referred to the proliferation of digital communications technologies that were becoming increasingly difficult for the FBI to penetrate and monitor in the due course of criminal investigations. Starting in 2022, and continuing today, Twitter has come under increasing scrutiny as evidence released by its new management indicates that the FBI has inappropriately commandeered a troubling degree of control over first amendment protected user content published by American citizens on Twitter. It is important to note that Sharp became Twitter's first in history U.S. Government liaison only one year after Judge Caproni's discussion of the FBI's concerns on C-SPAN3. In December 2022, Goodman released a comprehensive investigative report entitled "The Twitter Coup" **(EXHIBIT F)** in which he details well founded

allegations that suggest an inappropriate, hidden relationship between Judge Caproni, Sharp, the FBI, and Twitter that was not disclosed during the case giving rise to the forthcoming 60(b)(3) motion alleging newly discovered fraud.

VIII. Nina Jankowicz and the DHS Disinformation Governance Board

On or about April 27, 2022, Department of Homeland Security Secretary Alejandro Mayorkas announced the creation of the Disinformation Governance Board and the appointment of Executive Director Jankowicz. Many Americans bristled at the announcement finding the concept of a government agency policing social media content and subjectively rejecting first amendment protected speech that Jankowicz found "lawful but awful" to be a gross abuse of power and fundamentally unconstitutional. Goodman was one of those people. No process was defined for adjudicating exactly what Jankowicz determined to be information or disinformation. By all measures the determination appeared to be arbitrary and left to Jankowicz in her sole discretion. Goodman published an investigative report on a YouTube channel established after the destruction of the Jason Goodman channel ("Crowdsource the Truth 5") on or around May 16, 2022. The report contained information and evidence related to Jankowicz and her role at DHS. Specifically, Goodman discovered public fillings made by Jankowicz that appeared to indicate she was receiving funds from foreign non-profit organizations funded by the British, Canadian, and Italian governments while she was working for the U.S. Government and policing the first amendment protected speech of American citizens. Goodman's broadcast asked the fundamental question why Jankowicz was not registered as a foreign agent pursuant to 22 U.S. Code § 612, the Foreign Agent Registration Act ("FARA"). The following day, the video was permanently removed from YouTube, along with Goodman's Crowdsource the Truth 5 channel

with its over 10,000 subscribers. Separately, on the same day, a fraudulent complaint was filed with Patreon in violation of 18 U.S. Code § 1343, alleging Goodman had violated the rules against publishing private information. Two days later on May 18, 2022, Secretary Mayorkas announced the dissolution of the board and Jankowicz' resignation. (https://www.cnn.com/2022/05/18/politics/dhs-disinformation-board-paused/index.html).

Jankowicz claimed she had been the victim of disinformation but did not cite Goodman's reporting and neither she nor the DHS denied Goodman's claims or refuted the evidence he presented. Goodman alleges Jankowicz conspired with Sweigert to strategically attack Goodman's Patreon account. Sweigert is specifically aware this account is used to process credit card payments and represents a substantial portion of Goodman's annual income. For years, Sweigert has threatened Patreon with frivolous legal action related to Goodman's posts on the site. It is unlikely Jankowicz would be aware of the comparatively obscure Patreon account and its inherent value to Goodman without being informed by Sweigert. Sweigert's own web page features a photo of Jankowicz along with the message "call me". **(EXHIBIT G)**

Goodman did not post personal information, nor did he post disinformation. Goodman presented information contained in public filings he obtained from business records available on websites hosted by the Virginia Secretary of State and others, voluntarily filed by Jankowicz. In November 2022, Jankowicz returned to public view when the UK funded Centre for Information Resilience announced they had hired Jankowicz and that she had registered as a foreign agent, **(EXHIBIT H).** This sequence of facts further supports Goodman's allegations regarding Jankowicz. Goodman's primary business Twitter account ("@csthetruth") which was followed by nearly 30,000 Twitter users had been permanently suspended due to the malicious efforts of

Bouzy and Sweigert's Cyber Militia members on or around March 18, 2022, in retaliation for filing this lawsuit and in violation of 18 U.S. Code § 1513. **(EXHIBIT I)**

The account was reactivated under the new policies of Twitter's new management in January 2023. Within hours of reactivation, Goodman posted several links to Crowdsource the Truth videos that resulted in four new paid subscribers the same day, further demonstrating the proximate damage caused by deliberate deactivation of Goodman's social media accounts. Goodman also posted a link to his original report concerning Jankowicz' failure to register as a foreign agent while employed by DHS and her subsequent November 18, 2022, FARA registration that confirmed Goodman's initial reporting. Despite the fact that the FARA unit explicitly states that it makes registration information available to the public to inform the public about the activities of foreign agents within the United States, Jankowicz reiterated her fraudulent claim and filed a complaint with Twitter alleging Goodman had posted private information. Jankowicz' claim resulted in the re-suspension of @csthetruth which remains deactivated today despite numerous appeals citing 22 U.S. code § 612 and its legal requirements.

Goodman alleges Jankowicz specifically calculated this fraud to conceal facts that U.S. citizens have a legal right to know and that she would have further coordinated with Sweigert and or Bouzy to violate Goodman's first amendment rights and increase damage to Goodman's business property by informing Twitter to ignore the well-founded appeal and citations of law, by wrongfully deactivating @csthetruth once again. **(EXHIBIT J)**

This violation of 18 U.S Code § 1343 is another element in the consistent pattern of racketeering the Enterprise has engaged in over the past five years with the express intent of harming Goodman. The tweet posted by Goodman contained a URL link to Jankowicz' own

public filing which included the address of a P.O. Box at a UPS Store in Arlington Virginia and not Jankowicz's personal address. Even if Goodman referenced a filing containing a home address or other personal information, the decision to include such information in a public FARA registration would convert it into public information and legally mandate its disclosure pursuant to the statute. Jankowicz deliberately deceived or otherwise coordinated with Twitter, with the express intent of harming Goodman and in violation of law, for the purpose of seeking revenge against Goodman for revealing true facts that were disfavored by Jankowicz.

FIRST CAUSE OF ACTION

Fraud

52. Plaintiff incorporates by reference each and every allegation set forth in the preceding paragraphs as if fully stated herein.

53. Defendants caused a fraudulent pleading to be transmitted to the U.S. District Court for the MIED in violation of 18 U.S. Code § 1343, 18 U.S. Code § 1503, and 18 U.S. Code § 1513 when Loury altered the date of a pro se pleading filed with the Court on June 21, 2021, attributed to Webb but authored by Loury at Sweigert's direction.

54. In furtherance of their fraud, Defendants brought legal action and submitted pleadings over the internet violating 18 U.S. Code § 1343 when Webb sued alleging privileged statements made in an Amicus Curiae brief were defamatory but provided no evidence to refute the well-founded allegations of document forgery and fraud.

55. Plaintiff suffered special damages as a proximate cause of Defendant's fraudulent representations and malicious actions when he was compelled to travel to Detroit,

Michigan at his own expense to attend a hearing directly related to Defendants' fraudulent acts at the orders of Judge Gershwin Drain and additional costs and fees.

56. Defendant Sharp violated 18 U.S. Code § 1343 when he transmitted a false statement to YouTube over the internet in the form of a fraudulent copyright infringement complaint that he knew to be false at the time. Sharp did this with the express intent of depriving Goodman of his property in the form of software and intellectual property Goodman stored on YouTube. Sharp engaged in this fraudulent behavior for the express purpose of damaging Goodman and denying access to property.

57. Defendants Sharp, ATAS, and Esquenet participated in a scheme to commit fraud on the Court in violation of 18 U.S. Code § 1343 by initiating fraudulent litigation for an improper purpose when they sued Goodman's corporation in The National Association of Television Arts and Sciences v Multimedia System Design with the express intent of wrongfully denying Goodman his right to a fair trial, denying his access to the courts and denying his right to defend himself pro se.

58. Defendant Esquenet violated 18 U.S. Code § 1343 when she knowingly transmitted fraudulent pleadings to the Court in the course of litigation brough for a malicious purpose and the ulterior motive of damaging Goodman.

59. Defendants Sharp, ATAS, and Esquenet participated in a scheme to commit fraud on the Court in violation of 18 U.S. Code § 1343 by falsely claiming Sharp's private, for-profit corporation Sharp Things, LLC was inactive during the course of litigation in The National Association of Television Arts and Sciences v Multimedia System Design.

60. Defendant Jankowicz violated 18 U.S. Code § 1343 when she knowingly transmitted a fraudulent privacy complaint to Patreon.com over the internet with malicious intent to destroy Goodman's business property and terminate his access to a credit card payment processing account his subscription video business relied upon.

61. Defendant Jankowicz violated 18 U.S. Code § 1343 when she knowingly transmitted a fraudulent privacy complaint to Twitter.com over the internet with malicious intent to destroy Goodman's business property and terminate his access to a valuable branded social media account she knew Goodman's business relied upon.

SECOND CAUSE OF ACTION

Defamation

62. Plaintiff incorporates by reference each and every allegation set forth in the preceding paragraphs as if fully stated herein.

63. Defendants Webb, Sweigert and Bouzy defamed Goodman when they knowingly published false and defamatory statements about the Plaintiff to third parties on Twitter and elsewhere on the internet when they made claims likely to cause third parties to believe Goodman stood accused of raping Sports Illustrated supermodel Halima Aden, an individual who has never made such claims and who Goodman has never met.

64. Defendants Webb, Sweigert and Bouzy defamed Goodman when they knowingly published false and defamatory statements in general that accused Goodman of rape when they knew such statements to be false and inherently damaging per se libel.

65. The Defendants made these statements to third parties knowing they were false and without privilege, while deliberately ignoring the true facts of the matter.

66. Defendants made these statements with actual malice, and with intent to expose Goodman to public hatred and loss of professional and personal reputation with the express intent of damaging Goodman in his business and profession.

67. Defendant Bouzy defamed Goodman when he knowingly published false conclusory statements to third parties on Twitter declaring Goodman had falsely accused Wittes of deliberately misleading the public with regard to the death of Peter W. Smith.

68. Defendant Bouzy made these defamatory statements with the full knowledge that Goodman is a professional investigative journalist and his reputation for truthfulness is inherently valuable in his profession.

69. Defendant Bouzy made these statements even though he himself agreed in a phone call that the death was suspicious and the police investigation was superficial.

70. Defendant Bouzy made these statements with actual malice and the express intent of damaging Goodman in his professional reputation and causing proximate pecuniary damages to Goodman.

71. At the time the Defendants made the statements, they knew the statements to be false and defamatory or alternately, chose to deliberately ignore the truth.

72. Defendants made these false and defamatory statements with actual malice, and the express intent to malign and injure the Plaintiff.

73. Defendant Bouzy has hundreds of thousands of Twitter followers, dozens of which read, and acknowledged or responded to Defendants' false and defamatory statements clearly indicating they had been published to third parties without privilege or authorization.

THIRD CAUSE OF ACTION

Abuse of Process

74. Plaintiff incorporates by reference each and every allegation set forth in the preceding paragraphs as if fully stated herein.

75. Defendant Sweigert abused regularly issued civil process with the intent to harm Goodman without a legitimate excuse or justification, and perverted use of the process to achieve the collateral objective of destroying Goodman's business and overwhelming him with vexatious litigation when he brought multiple civil actions and attempted to intervene in existing civil actions against Goodman across a wide range of U.S. District Courts including South Carolina, the Southern District of New York, the Eastern District of Michigan and the Eastern District of Virginia.

76. Defendant Sharp abused regularly issued civil process with intent to harm Goodman when he endeavored to create a fraudulent excuse in his wrongful attempt to justify vexatious litigation against a company owned by Goodman for a parody image posted on the internet by Goodman in violation of 47 U.S. Code § 230. Sharp perverted the use of the process and applied the power of the Court in a manner not intended by the law to achieve the collateral objective of destroying Goodman's popular subscription video service for the improper purpose of preventing Goodman from broadcasting during the 2020 election. Sharp did this with malicious intent and for the improper purpose of his own political and financial benefit and that of his preferred Presidential candidate.

77. Defendants violated 18 U.S. Code § 1503 when Sweigert harassed Snyder, the attorney retained to represent Goodman's corporation. Defendants abused regularly

issued civil process with intent to harm Goodman for the express purpose of denying him the right to a fair trial and the right to defend himself pro se causing proximate harm to Goodman in the form of significant financial damages, damages to his business and reputation, and loss of property in the form of his valuable branded social media accounts that his business relied upon.

Fourth Cause of Action

Civil Conspiracy

78. Plaintiff incorporates by reference each and every allegation set forth in the preceding paragraphs as if fully stated herein.

79. Defendants Sweigert, Sharp, ATAS, and Esquenet entered into a civil conspiracy when they agreed to create a pretext under which they intended to sue a corporation owned by Goodman for an internet post made by Goodman in his personal capacity in violation of 47 U.S. Code § 230 and with the express intent of harming Goodman and extorting him into ceasing news broadcasts during the 2020 Presidential election.

80. In furtherance of the civil conspiracy, Sweigert caused an email to be sent from an allegedly anonymous email address in violation of 18 U.S. Code § 1343 with the express intent of creating a pretext for a lawsuit against a corporation owned by Goodman that Sharp, ATAS, and Esquenet had no knowledge of prior to entering the conspiracy with Sweigert. The conspiracy caused acute proximate pecuniary damage to Goodman by forcing him to retain an attorney who failed to defend Goodman's corporation according to Goodman's instructions and then withdrew as a direct result of harassment by the

Enterprise. Defendants calculated their actions specifically to harm Goodman or otherwise should have known his injuries were a foreseeable result of their conspiracy.

81. Defendants Webb and Sweigert entered into a civil conspiracy with non-party Loury in violation of 18 U.S. Code §§ 1343 and 1513 when they caused a fraudulent document to be filed with the Court in the Eastern District of Michigan.

82. Defendants did this with the express intent of harming Goodman by denying him his rights to a fair trial and with the express intent of damaging Goodman with costs and fees associated with defending malicious, vexatious litigation.

83. Defendants committed this overt act, knowing the case would otherwise be dismissed if not for the conspiracy to file the fraudulent document. Defendants proceeded with the full knowledge that their actions would proximately damage Goodman and they did so with malicious intent.

84. Defendants knew or otherwise should have known the actions of their conspiracy would harm Goodman in the form of pecuniary damages due to burdensome litigation.

85. Defendants Sweigert and Webb engaged in a pattern of racketeering activity beginning in 2017 and including the creation and operation of an association in fact enterprise consisting of multiple individuals including each Defendant and additional non-parties to this case.

86. Defendants Sweigert and Webb engaged in a pattern of racketeering activity, which included extortion, and fraud, with the express intent of harming Goodman.

87. Defendants Sweigert and Webb enlisted each of the other defendants to cooperate with them for a common purpose and towards a common goal of damaging Goodman and wrongfully denying him access to his property.

88. The Defendants racketeering was proximately related to the Enterprise and furtherance of the various conspiracies it engaged in as set forth herein.

89. The Defendants' racketeering activity affected interstate commerce by proximately damaging Goodman in the state of New York while utilizing coconspirators in New Jersey, Connecticut, Washington D.C. and other states and also through the transmission of false statements over the wires of the internet and or phones to service providers and social media platforms in California, Wyoming and New Hampshire.

90. Defendants Webb, Bouzy and Jankowicz at a minimum, derived income as a direct or indirect result of their participation in the Enterprise.

91. Defendant Wittes invested money derived directly or indirectly from his involvement with the Enterprise when he financed the civil defense of Bouzy and Bot Sentinel by retaining Ballard Spahr attorneys Berlin and Mishkin.

92. Plaintiff Goodman suffered reputational damage and substantial pecuniary damage to his business and his valuable branded social media properties as a proximate result of the Defendants' racketeering activity.

PRAYER FOR RELIEF

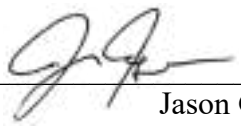
WHEREFORE, Plaintiff prays the Court will enter judgement in his favor and issue an order for the following relief:

1. Declaring that the Defendants statements were libelous and defamatory.

2. Declaring Defendants vexatious litigants and mandating that each first seek leave of this Court before bringing future litigation against Goodman or any company owned or utilized by Goodman effective immediately and on into perpetuity.
3. Granting an order compelling Defendants ATAS, Sharp and Esquenet to issue a public apology to be approved by Goodman prior to publication admitting to their wrongdoing and absolving Goodman and MSD of false claims. The release is to be issued in the Hollywood Reporter, Variety, and Bloomberg Law and must occupy at least as much editorial space as the September 4, 2020 article entitled "Television Academy Sues After Emmy Statuette Given Coronavirus"
4. Granting Goodman relief for money damages for all economic losses including, but not limited to, lost past and future earnings; and for compensatory damages; and for punitive damages; and for interest at the maximum legal rate on all sums awarded; and for such other and such further relief as the Court deems just and proper.

Signed this 17th day of January 2023

Respectfully submitted,



Jason Goodman, Plaintiff, Pro Se
252 7th Avenue Apt 6s
New York, NY 10001
(323) 744-7594
truth@crowdsourcethetruth.org

(EXHIBIT A)

son Goodman George Webb Cyber
alking Alt-Right DEFANGO Robert
avid Steele Larry Klayman

Home New Page Blog

All Posts

Log in / Sign up

#SDNYORG
Jan 4 1 min

[SDNY] Hindenburg Lawfare: the Jason Goodman v. Chris Bouzy disaster court files

[SDNY] SDNY court described "conspiracy theorist" who "sounds like Q-Anon" and "traffics in conspiracy theories" that are...

474 views 0 comments 21

#SDNYORG
Nov 4, 2022 3 min

[SDNY] Jason Goodman's mysterious choking attack, "we have no record" says NYPD

ABOVE: JASON GOODMAN (POLICE SNITCH) REVEALED TO CHARLES ORTEL (11/6/22) THAT IT WAS HE (HIMSELF) THAT SUMMONED NYPD PATROL...

2,585 views 1 comment 41

#SDNYORG
Oct 23, 2022 4 min

[SDNY] Tavistock social engineering exposed by #LAWTUBE lawyers guided by Jason Goodman

[SDNY] TWENTY SECOND DAY OF
GARDEN VARIETY CRAZY CONSPIRACY THEORIST

Let's Chat!

JASON "CREEPO" GOODMAN (PRESENTLY ON THE…

3,127 views 0 comments 53

#SDNYORG
Oct 16, 2022 2 min

[SDNY] #LAWTUBE rape culture in Chris Bouzy, Jason Goodman and George Webb lawsuit

[SDNY] SIXTEENTH DAY OF OCTOBER 2022. JUST AFTER GEORGE WEBB CELEBRATED HIS BIRTHDAY, HE WAS ON A PLANE TO SANTA MONICA, CALIF TO…

2,887 views 0 comments 54

#SDNYORG
Oct 9, 2022 3 min

[SDNY] Rape allegations won't go away for Jason Goodman and Chris Bouzy SDNY lawsuit

[SDNY] NINTH DAY OF OCTOBER 2022. INTERNET SHOCK WAVES CRASHED AMONGST THE #LAWTUBE AND #LAWFARE COMMUNITIES ABOUT THE SLAP…

2,954 views 0 comments 50

#SDNYORG
Oct 7, 2022 1 min

[SDNY] Fans fear Jason Goodman may slip into a depression after the loss of Puff the Magic Dragon

[SDNY] SEVENTH DAY OF OCTOBER 2022. GRIEF STRICKEN NEW YORKER CONSPIRACY THEORIST TOOK TO HIS BROADCAST TO HOLLYWOOD,…

1,955 views 0 comments 46

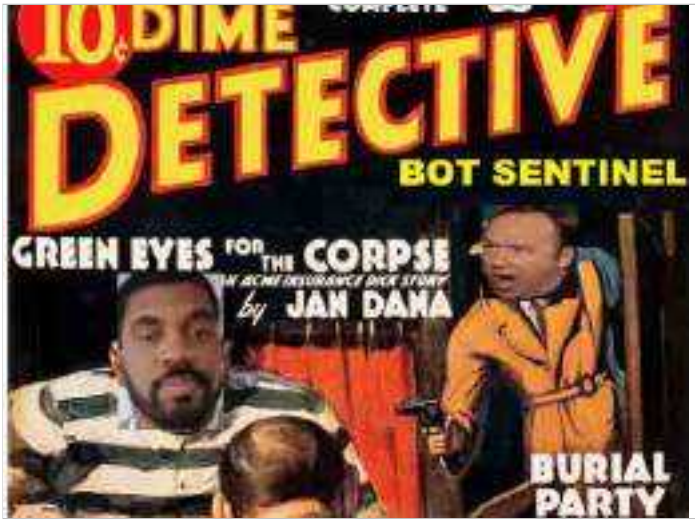
#SDNYORG

Oct 3, 2022 2 min

[SDNY] TWITTER BUFFS ZERO IN ON "VITAL COUNTER POLICY" DEFENSE FOR CHRIS BOUZY - BOT SENTINEL

[SDNY] FIFTH DAY OF OCTOBER 2022. INTERNET RUMORS POINT OUT THAT JASON GOODMAN HAS EFFECTIVELY DISAPPEARED FROM THE STREETS OF...

2,205 views 0 comments 48



#SDNYORG
Sep 29, 2022 4 min

[SDNY] FURIOUS LARP LAWFARE AS CHRIS BOUZY FOLLOWS CEASE AND DESIST SCRIPT

[SDNY] THIRTIETH DAY OF SEPTEMBER 2022. THE INTELLIGENCE COMMUNITY'S APPARENT SECOND ATTEMPT AT A SHOW TRIAL PSYOP SEEMS TO BE...

1,871 views 0 comments 48

#SDNYORG
Sep 28, 2022 3 min

[SDNY] New Jersey Attorney General apparently getting privacy complaints about Chris Bouzy

[SDNY] TWENTY EIGHTH DAY OF SEPTEMBER 2022. THOUSANDS OF SUPPORTERS ARE BURNING UP THE INTERNET BLOGOSPHERE WITH OUTRAGE OVER...

1,864 views 0 comments 45

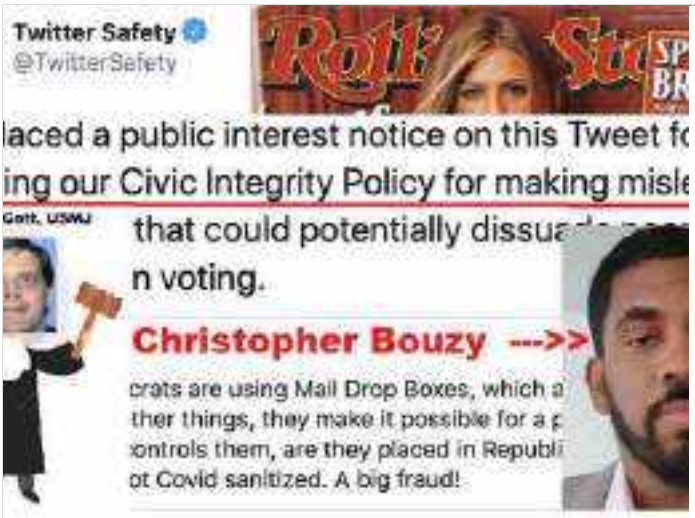
#SDNYORG
Sep 27, 2022 2 min

[SDNY] Deja Vu "LawTube" community aflame with Chris Bouzy & Bot Sentinel vicarious liability talk

[SDNY] TWENTY SEVENTH DAY OF SEPTEMBER 2022. TWITTER TERMINATED THE ACCOUNT OF A

"LAWTUBE PERSONALITY" FOR "REKIETA LAW" (122K...

2,180 views 0 comments 46



#SDNYORG
Sep 25, 2022 2 min

[SDNY] Jason Goodman enemy Christopher Bouzy in lawsuit firestorm over Twitter fraud

[SDNY] BREAKING [TWENTY FIFTH DAY OF SEPTEMBER 2022] BLITZKRIEG LEGAL FORCES READY TO POUNCE ON CHRISTOPHER BOUZY AND HIS BOT...

2,473 views 0 comments 44

#SDNYORG
Sep 12, 2022 3 min

[SDNY] Virginia court rules against Jason Goodman, Robert David Steele lawsuit moves forward

BREAKING: SIXTEENTH DAY OF SEPTEMBER, 2022. The Robert David Steele lawsuit in the Eastern District of Virginia will proceed ahead...

8,740 views 0 comments 50

#SDNYORG
Sep 9, 2022 2 min

[SDNY] Crazy Conspiracy Theorist Jason Goodman exploiting more insane viewers on 9/11-THON for cash

WARNING TO THE PUBLIC BREAKING: [NINTH DAY OF SEPTEMBER, 2022, NEW YORK CITY] CONSPIRACY THEORIST JASON GOODMAN PREPARES TO ROLL-OU...

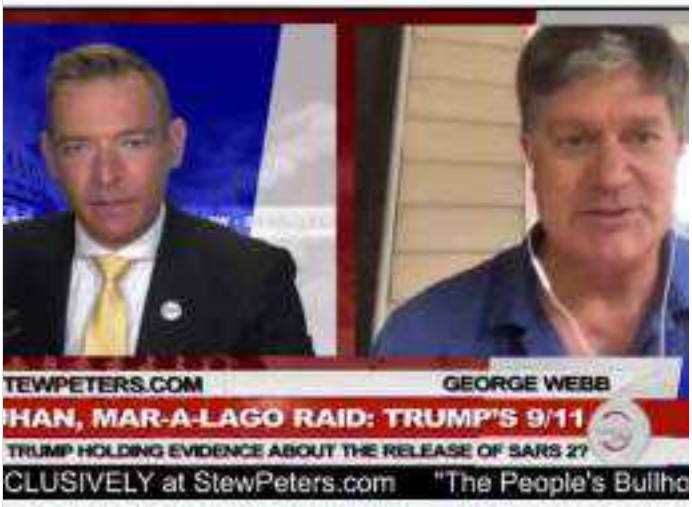
6,039 views 0 comments 54

#SDNYORG 3 min

[SDNY] LBRY, INC., ODYSEE HOLDINGS, INC., and Jason Goodman to be sued for racketeering

EXECUTIVE SUMMARY "Radicals post specifically on platforms such as Odyssey, Bitchute, and Steam It is a strategy of the new right and ...

6,880 views 0 comments 61



#SDNYORG
Sep 4, 2022 3 min

[SDNY] George Webb's efforts to obtain Special Master for Trump explained in Atlanta federal court

BREAKING: George Webb has largely claimed responsibility for the appointment of a Special Master to oversee the classification of...

7,958 views 0 comments 59

#SDNYORG
Aug 31, 2022 2 min

[SDNY] PFC Patrick Bergy orbits possible Wall Street blood bath using I.I.A. software on 9/11/2022

THE COMING NEW DARK AGES THE EDITORIAL BOARD OF SDNY.ORG IS PROVIDING INFORMATION TO LAW ENFORCEMENT THAT HAS BEEN COLLECTED FROM...

9,499 views 0 comments 58

#SDNYORG
Aug 24, 2022 3 min

[SDNY] The dark figures of Odysee and LBRY exposed by REUTERS -- Jason Goodman poster child

[SDNY, NEW YORK CITY, 8/24/2022]. A REUTERS

INVESTIGATION INTO WACKO CRYPTO CURRENCY FIRMS LBRY AND ODYSEE CONFIRMS REPORTING OF...

9,714 views 0 comments 59

#SDNYORG
Aug 4, 2022 1 min

[SDNY] Crypto's LBRY, Inc and the skeleton in the closet of Josh Finer, MBA ("the well born few")

BREAKING: THE CRYPTOCURRENCY COMMUNITY IS ASKING QUESTIONS ABOUT KEY LEADERSHIP IN THE NEW HAMPSHIRE BASED LBRY, INC. AS THE U.S....

8,127 views 0 comments 66

#SDNYORG
Aug 1, 2022 1 min

[SDNY] Should NYC issue a concealed gun permit to alleged sadist Jason Goodman of Chelsea

BREAKING: NEW YORKERS ARE BRACING FOR THE POSSIBILITY THAT A CONCEALED WEAPONS PERMIT MAY BE ISSUED TO ALLEGED MISCONDUCT WITH...

7,076 views 0 comments 65

#SDNYORG
Jul 27, 2022 3 min

[SDNY] Jason Goodman ordered to Detroit by Judge Gershwin Drain -- road trip from hell

BREAKING: JASON "SNEAKY" GOODMAN MUST APPEAR, WITH AN ATTORNEY, BEFORE JUDGE GERSHWIN DRAIN IN THE MICHIGAN EASTERN...

5,346 views 0 comments 67

-
Jul 24, 2022 1 min

[SDNY] Russian doomsday agents run lawsuit cover-up of Crimean-Congo hemorrhagic fever outbreak

BREAKING: Crimean-Congo hemorrhagic fever (CCHF) outbreak in Spain, right on cue, miraculously predicted by the dynamic duo of Russian...

4,217 views 0 comments 64

-
Jul 21, 2022 1 min

[BREAKING] - MASS ARRESTS PLANNED FOR CLERK OF COURT STAFF AUGUST 4TH, FREE HOT DOGS

BREAKING - ACCORDING TO INTERNET RUMORS AT LEAST A DOZEN STAFF MEMBERS OF THE U.S. DISTRICT COURT IN DETROIT MICHIGAN FACE...

3,283 views 0 comments 52

-
Jul 20, 2022 2 min

[SDNY] Jason "Peter Pansexual" Goodman faces doom after George Webb's Meghan "Crazy Ivan" Markle

BREAKING: DETROIT JUDGE STRIKES ALL OF JASON GOODMAN'S COURT FILINGS AND ORDERS HE OBTAIN AN ATTORNEY. ABOVE: Detroit judge Gershwin...

2,838 views 0 comments 51

-
Jul 18, 2022 1 min

[SDNY] Over-confident Jason "Peter Pan" Goodman blind-sided by George Webb's change of venue

BREAKING: George Webb files a CHANGE OF VENUE

BREAKING: George Webb files a CHANGE OF VENUE motion in his lawsuit against Jason "hate monger" Goodman. "Pure heart - empty head"...

2,635 views 0 comments 48

-
Jul 16, 2022 2 min

[SDNY] BREAKING: GEORGE WEBB TELLS JUDGE HE HAS COVID-19 TO AVOID JASON GOODMAN

BREAKING: S.D.N.Y. MAGISTRATE JUDGE, BARBARA MOSES, WON'T ROLL OVER LIKE A CRAZED GEORGE WEBB FAN (SLANG = CAT LADIES). GEORGE WEBB...

2,571 views 0 comments 43

-
Jul 12, 2022 1 min

[SDNY] Federal Judge Valerie E. Caproni throws Jason Goodman's lawsuit in the trash bin

BREAKING: "Counter Lawfare" guru Jason "Karen" Goodman has had yet another frivolous federal lawsuit dismissed by Judge Valerie E....

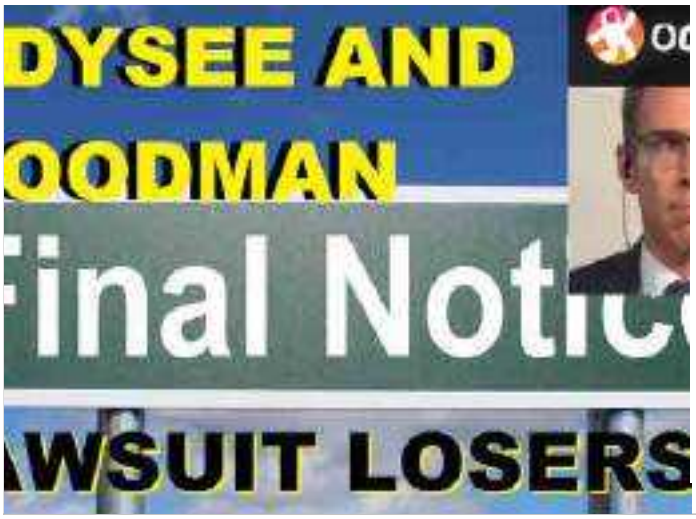
1,952 views 0 comments 44

-
Jul 10, 2022 4 min

[SDNY] GETTR lawsuit over Jason Goodman's videos heats up -- another ODYSEE default?

Conspiracy Theorist laughs off another lawsuit New York City's own hyper-aggressive meter maid, Jason Goodman, seemed to laugh off...

2,072 views 0 comments 46



-
Jul 8, 2022 1 min

[SDNY] Jason Goodman and ODYSEE now in default -- Mr. Counter Lawfare Fail

NOTICE BY PUBLICATION MULTIMEDIA SYSTEM DESIGN, INC. C.E.O. JASON GOODMAN, AND ODYSEE HOLDINGS, INC. ARE THE SUBJECT OF AN ENTRY OF...

1,621 views 0 comments 44

-
Jul 5, 2022 1 min

[SDNY] Christopher Bouzy releases the lawyer hounds on ole' Jason Goodman - NOW IN DEFAULT

BREAKING: Jason "Karen" Goodman's company in DEFAULT, Multimedia System Design, Inc. BREAKING: Proof that Christopher Bouzy has...

903 views 0 comments 44

-
Jun 30, 2022 5 min

[SDNY BOMBSHELL] GEORGE WEBB FACES DEALEY PLAZA ON 7/20/2022 IN S.D.N.Y. (DALLAS)

BREAKING: U.S. SUPREME COURT ADVISED OF POSSIBLE CRIMINAL COLLUSION OF S.D.N.Y. MAGISTRATE JUDGES BARB C. MOSES AND STEWART...

612 views 0 comments 52

-
Jun 26, 2022 2 min

[SDNY] PATREON walks into so-called litigation chainsaw with allegations of racketeering

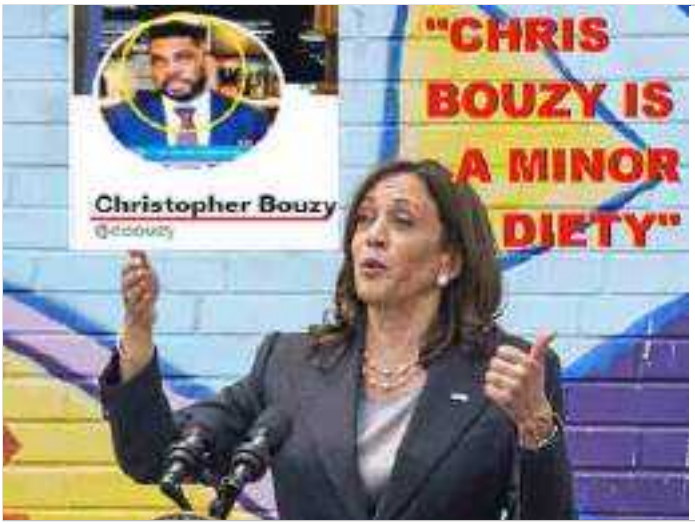
The cultish San Francisco Millennials that run the "tree house" at PATREON (a potential Securities and

-
Jun 22, 2022 4 min

[SDNY MORGUE] Jason Goodman's trail of mental health incidents: terrorizing women

This August 13th marks the fourth anniversary of the death of investigative journalist Jenny Marie Moore. What were her connections to...

764 views 0 comments 45



-
Jun 19, 2022 1 min

[SDNY WHITE HOUSE] Vice President's Task Force gets FULL REPORT on MEGHAN MARKLE

WARNING: ANY ATTACKS ON THE BOT SENTINEL, INC. SERVERS WILL BE MONITORED BY PRIVATE INTELLIGENCE CONTRACTORS TO PREVENT ANY...

256 views 0 comments 41

-
Jun 15, 2022 3 min

[SDNY] Kamala Harris Task Force will be fully briefed on Christopher E. Bouzy and George Webb

OPINION AND EDITORIAL The Office of the President of the U.S. Senate is presently receiving files and dossiers of key court documents as...

770 views 0 comments 48

-
Jun 13, 2022 1 min

[USCG] Have a good "dirty bomb hoax" laugh at the Port of Charleston on June 14th, 2017

It was five years ago today (June 14, 2017) that the bungling and inept knuckle draggers at U.S. Coast Guard District Charleston created...

158 views 0 comments 34

-
Jun 6, 2022 5 min

[SDNY ALERT] SPUTNIK wife beater Lee Stranahan loses defamation lawsuit, can you spell l o s e r ?

BREAKING: LINGERING QUESTIONS ABOUT POSSIBLE DOMESTIC VIOLENCE ARREST OF LEE STRANAHAN ABOVE: Prior to his move to Sioux Falls, South...

577 views 0 comments 49

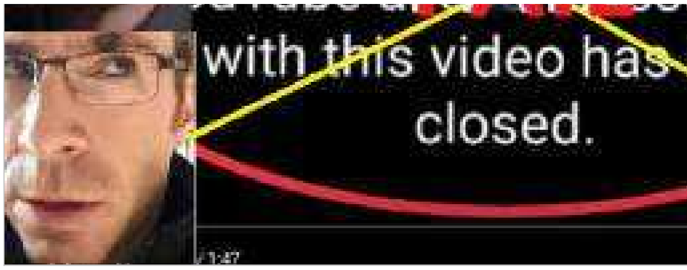
-
May 29, 2022 5 min

[RUSSIAN DOOMSDAY] IS A NUCLEAR EVENT, A LA PORT OF CHARLESTON, IN OUR FUTURE?

U.S.C.G. ADMIRAL LINDA L. FAGAN ASLEEP AT THE HELM America's ports remain vulnerable to continued "dirty bomb hoax" attacks that may...

539 views 0 comments 40

-
May 26, 2022 2 min



[ALERT SDNY] Russian friendly Jason Goodman kicked off YouTube -- two more channels term'ed

BREAKING The social media channels of alleged Hollywood sexual pervert and possible Russian disinfo

-
May 22, 2022 1 min

[ALERT SDNY] Judge issues orders in "Amber Heard" Christopher E. Bouzy @cbouzy lawsuit

Christopher E. Bouzy is the new darling of the Amber Heard "bot attack" press frenzy. Perfect timing for the Magistrate Judge in Jason...

399 views 0 comments 35

-
May 18, 2022 1 min

[ALERT DHS] JASON GOODMAN REPORTED TO FEDS -- 3 TWITTER ACCOUNTS TERM'ED

Racist bigot Jason Goodman reported to the Federal Bureau of Investigation. Twitter terminated "Sneaky" Goodman's three (3) Twitter...

258 views 0 comments 35

(EXHIBIT B)

Scott Anthony Archives: Politics, Government Affairs, Congressional Hearings, Healthcare, Foreign Affairs

Search The Archives

Search

Sunday, June 11, 2017

Researchers Being Attacked By Crowdsource The Truth Member Jason Goodman: Credibility Called Into Question

Good morning,

Today is Sunday, June 11, 2017.

I am providing this video and a written response as a matter of public record, in response to a video uploaded and broadcast on the social media platform YouTube on this date approximately four and a half hours ago, entitled "Deep State Attack on George Webb & Crowdsource the Truth".

Like almost all of you watching this video, and indeed, the ones uploaded by either George Webb or Jason Goodman and any subsequent livestreams either individually or collectively (also known as "Crowdsource the Truth" hereinafter referred to as CTT), I believe that we all would like to see the rapid apprehension and prosecution for the persons responsible for either the murder or disappearance of the individual we have come to know as "Seth Rich". For many, the story of Seth Rich and his alleged homicide evokes a visceral reaction for justice. I concur with the need for justice in the case of any unsolved homicide, abduction, or any other capital offense or felony. After all, we are a "nation of laws" in the United States of America, and it is woven within our founding father's words of wisdom that all people shall enjoy "Life, Liberty and the Pursuit of Happiness".

Disturbingly, on this date, and prior to this date, a trend had been developing on both Mr. Webb's and Mr. Goodman's channels and the videos they have been uploading: what had at first seemed like a novel idea to "storyboard" and "crowdsource" an open investigation into potential crimes committed against innocent Americans by a host of entities and individuals that have been named by Mr. Webb and Mr. Goodman within their video content, has crossed into the realm of what I consider highly unethical, dangerous, and potentially illegal behavior. It is for these reasons that I can no longer sit idly by as Mr. Webb and Mr. Goodman utilize various psychological tactics to illicit responses from their viewers.

While Americans enjoy a "Free Press" and the right to ensure that those who have committed crimes are held accountable, there are well established methods and processes to ensure that information is accurately reported, and those accused of potential crimes are afforded due process. In America, we are free to say what we like, without fear or prejudice, as long the safety of others or their civil rights is not violated. Regarding the Rule of Law however, there are a host of safeguards in place to ensure that the right person is tried for the right crime and is judged by a jury of their peers utilizing constitutional protections. For this reason, and almost this reason alone, America has been one of the beacons of liberty around the globe since our nation was founded.

In the video broadcast earlier today, Jason Goodman issued what I believe was designed to be a "call-to-action" video: that is, he created it with the intent to utilize psychological tactics to illicit a response. The average person may not be aware such tactics are being utilized. This is understandable as they are very subtle by design. I believe the purpose of Jason's video was to encourage others to start investigating a person known on YouTube as "Defango", also known as Manuel Chavez. However, there are implied messages as well, as you will see throughout this call-to-action video. This is how I perceived the messaging in the above named video, and while it is impossible for me to state with certainty that was Mr. Goodman's intent, perception is reality in many instances. Thus, a reasonable person may likely draw the same conclusions I have regarding the intent of his video.

It should be noted that while Mr. Goodman has made it clear that his relevant employment history and experience is comprised of the creation of 3D Stereoscopic cameras and/or other inventions for Hollywood filmmaking, Mr. Goodman has never indicated former employment or experience in the fields of journalism, law enforcement, or the legal profession at large. This is an important distinction because he very likely lacks the fundamental and basic education required to conduct a large-scale investigation into criminal activities as the CTT library entails. It should also be noted that at no time have I witnessed Mr. Webb state that he possesses the requisite professional training to conduct criminal investigations in the same manner.

In reviewing the library and archived video evidence that both Mr. Webb and Mr. Goodman have catalogued on their channels, there is ample evidence that lack of appropriate training in investigations and law enforcement easily places the public at risk. In no particular order, and by no mean a comprehensive list, some of the more obvious issues may be:

1. Implicating or accusing an innocent person of wrong-doing, including being part of a criminal conspiracy;
2. Revealing the identity of an otherwise private individual with no knowledge of the investigation to the Crowdsource audience;
3. The potential for over-eager and inexperienced "researchers" to commit acts of harassment towards innocent persons;
4. The potential for large numbers of viewers to contact family, friends, co-workers of the stated victims (which would fall under the aforementioned harassment issue)
5. The potential for inexperienced investigators to place themselves into dangerous scenarios during the canvassing and interviewing of potential witnesses;
6. Exposing actual witnesses of a criminal investigation where their protection might otherwise be afforded by law;
7. The inherent lack of ability to control the direction of the investigation, all of which could compromise or undermine actual investigations currently underway

In contrast, I am publishing this as a matter of record from the viewpoint of a person who has been employed as a law enforcement

official, although it is not my current profession. Currently, I am licensed and Board Certified healthcare practitioner able to assess and treat conditions, injuries, and illnesses across the age spectrum, including mental health. It is both my prior and current occupations that afford me the insight, formal training, and ability to detect even subtle nuances in the human condition the average person might overlook.

I understand that my assessment will be met with resistance from many. I accept that many of you will continue to follow Mr. Goodman and Mr. Webb regardless of the information I provide. However, it is my hope that those who may feel compelled to take any actions against any individuals named within this video, or any prior or subsequent videos that Mr. Webb, Mr. Goodman, or their "Associates" produce and publish, will pause and think through the ramifications if the actions taken are based off of faulty investigative techniques, lack of appropriate citations, sources and methods during their investigation, and not least of all, the potential criminal and civil rights violations that might incur as a result of actions taken simply because Mr. Goodman has created a sense of urgency. The case of Seth Rich is nearing the one-year mark since the alleged crime has occurred. Urgency has long since passed, and this investigation is now in the long-haul phase where accurate and methodical law enforcement tactics should be used to bring those who committed the crimes against Seth Rich to justice.

Based on viewer reactions to the George Webb / Jason Goodman video series, and based on a variety of videos now being published, many of which touch upon the topic of what appears to be a somewhat reckless and potentially dangerous crowdsourced investigation process, it is my opinion that other individuals are detecting something amiss with the ethics of CTT's crowdsourced investigation.

Posted by Scott Anthony at 7:12:00 PM
Reactions:

Secure Connection Failed

An error occurred during a connection to web.archive.org

Links to this post
Email This BlogThis! Share to Twitter Share to Facebook Share to Pinterest
Labels: Agent19 , George Webb , Intelligence , Investigation , Jason Goodman , Montagraph , Online , Open Source , Persona , Review

Wednesday, June 7, 2017

Ex-FBI Director James Comey Releases His Opening Statement Prior To June 8th Hearing Before Congress

- BREAKING NEWS ITEM-
###

Statement for the Record
Senate Select Committee on Intelligence

James B. Comey

June 8, 2017

Chairman Burr, Ranking Member Warner, Members of the Committee. Thank you for inviting me to appear before you today. I was asked to testify today to describe for you my interactions with President-Elect and President Trump on subjects that I understand are of interest to you. I have not included every detail from my conversations with the President, but, to the best of my recollection, I have tried to include information that may be relevant to the Committee.

January 6 Briefing

I first met then-President-Elect Trump on Friday, January 6 in a conference room at Trump Tower in New York. I was there with other Intelligence Community (IC) leaders to brief him and his new national security team on the findings of an IC assessment concerning Russian efforts to interfere in the election. At the conclusion of that briefing, I remained alone with the President-Elect to brief him on some personally sensitive aspects of the information assembled during the assessment.

The IC leadership thought it important, for a variety of reasons, to alert the incoming President to the existence of this material, even though it was salacious and unverified. Among those reasons were: (1) we knew the media was about to publicly report the material and we believed the IC should not keep knowledge of the material and its imminent release from the President-Elect; and (2) to the extent there was some effort to compromise an incoming President, we could blunt any such effort with a defensive briefing.

The Director of National Intelligence asked that I personally do this portion of the briefing because I was staying in my position and because the material implicated the FBI's counter-intelligence responsibilities. We also agreed I would do it alone to minimize potential embarrassment to the President-Elect. Although we agreed it made sense for me to do the briefing, the FBI's leadership and I were concerned that the briefing might create a situation where a new President came into office uncertain about whether the FBI was conducting a counter-intelligence investigation of his personal conduct.

(EXHIBIT C)

Department of State
Division of Corporations

Entity Assumed Name History

Return to Results | Return to Search

Entity Details

ENTITY NAME: MULTIMEDIA SYSTEM DESIGN, INC.
FOREIGN LEGAL NAME:
ENTITY TYPE: DOMESTIC BUSINESS CORPORATION
SECTIONOF LAW: 402 BCL - BUSINESS CORPORATION LAW
DATE OF INITIAL DOS FILING: 06/21/1994
EFFECTIVE DATE INITIAL FILING: 06/21/1994
FOREIGN FORMATION DATE:
COUNTY: NEW YORK
JURISDICTION: NEW YORK, UNITED STATES

DOS ID: 1830828
FICTITIOUS NAME:
DURATION DATE/LATEST DATE OF DISSOLUTION:
ENTITY STATUS: ACTIVE
REASON FOR STATUS:
INACTIVE DATE:
STATEMENT STATUS: PAST DUE DATE
NEXT STATEMENT DUE DATE: 06/30/1996
NFP CATEGORY:

ENTITY DISPLAY | NAME HISTORY | FILING HISTORY | MERGER HISTORY | ASSUMED NAME HISTORY

Search

File Date	Assumed Name	Assumed Name ID	Status	Principal Location
10/10/2002	21ST CENTURY 3D	206900	Active	
05/15/1998	MULTIMEDIA SOFTWARE DESIGN	206899	Active	

Rows per page: 5 1-2 of 2

(EXHIBIT D)

Integration of cyber security incident response within holistic incident management systems to strengthen resiliency of the nation's critical infrastructure

Part two of a series
June 2013

Author: Dave Sweigert, M.Sci., CISSP, CISA, PMP

ABSTRACT

Response and recovery methods for severe cyber security incidents need traceable integration within incident management systems, which should be offered as a tool-set within the Executive Order 13636 Cybersecurity Framework.

Background

In September 2010, a 30-inch diameter natural gas pipeline exploded near a residential neighborhood of San Bruno, California. A fire followed which quickly engulfed nearby homes. As the site was two miles West of San Francisco Airport initial responders believed a jetliner had crashed in the area. It took the private operator, PG&E, 90 minutes to shut off the gas after the explosion.

Preventing severe incidents caused by technology is one of the goals of the White House as expressed in Executive Order 13636[1]. E.O. 13636 seeks to strengthen the protection of Critical Infrastructure and Key Resources (CIKR)[2], albeit via voluntary compliance with a new Cybersecurity Framework (CSF)).

E.O. 13636 seeks to "*explore the use of existing regulation to promote cyber security*" while "*understanding the cascading consequences of infrastructure failures..*[3]". This paper intends to meld both goals to better explore ways in which existing policy frameworks can be leveraged to further particularize the CSF with practical solutions.

[1] Executive Order -- Improving Critical Infrastructure Cybersecurity, 2/12/2013. See: Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure

[2] Critical Infrastructure: Assets, systems and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.
Key resources: Publicly or privately controlled resources essential to the minimal operations of the economy and the government.

[3] Presidential Policy Directive (PPD) 21

Industry check-box attitudes about cyber-security compliance

Although CSF is voluntary in nature, some private sector operators of CIKR have voiced their concern that severe incidents may require cohesive and coordinated rapid response and recovery, which is not addressed by technology-based standards (see responses to the U.S. National Institute of Standards and Technology (NIST), Request for Information (RFI)[4]).

Real CIKR resiliency may require examination of how an organization's response capabilities align with public or private partners and understanding those functional interdependencies.

In contrast, the Critical Infrastructure Protection (CIP)[5] Reliability Standards program (a Bulk Electric System (BES) industry[6] framework) has imposed a fine-based compliance scheme on the BES industry. CIP critics complain it is an administrative-based set of disjointed standards which foster a "check the box mentality" and has failed in achieving tangible "comprehensive and effective cybersecurity."[7]

To illustrate, the static CIP standard 009, "*Recovery Plans for Critical Cyber Assets*[8]", requires the creation of a "recovery plan" for "cyber assets". CIP-009 does not require integration of such a stand-alone recovery plan within the organization's overall severe incident response. So, cyber-incident escalation triggers that activate other response plans may or may not be addressed.

To be CIP-009 compliant, an entity only needs a cyber-incident response[9] plan to react to cyber hygiene focused events; e.g. sabotage reporting, privilege escalation, security perimeter breaches, etc. However, a response team may need visibility into the cascading consequences caused by network or system outages on critical infrastructure and may need to understand when and how to trigger a larger response to the unfolding event.

---

[4] Docket No. 130208119-3119-01, Industry responses to NIST Request for Information.

[5] North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Standards for Cyber Security

[6] http://www.nerc.net/standardsreports/standardssummary.aspx

[7] "Utilities are focusing on regulatory compliance instead of comprehensive security. The existing federal and state regulatory environment creates a culture within the utility industry of focusing on compliance with cybersecurity requirements, instead of a culture focused on achieving comprehensive and effective cybersecurity. Specifically, experts told us that utilities focusing on achieving minimum regulatory requirements rather than designing a comprehensive approach to systems security. In addition, one expert stated that security requirements are inherently incomplete, and having a culture that views the security problem as being solved once those requirements are met will leave an organization vulnerable to cyber attack. Consequently, without a comprehensive approach to security, utilities leave themselves open to unnecessary risk." United States Government Accountability Office, *Electricity Grid Modernization Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed* (Report to Congressional Requesters), GAO-11-117 (Washington, DC: U.S. Government Accountability Office, January 2011), 23,

http://www.gao.gov/products/GAO-11-117

[8] http://www.nerc.com/files/CIP-009-3.pdf

[9] Computer Security Incident Response Capability (CSIRC) or team (as defined within NIST Special Publication 800-61)

Alignment of the CIP-009 plan with other planning documents may be a prudent objective; e.g. integration with the Emergency Operations Plan (governed by yet another BES standard, the *EOP-001 Emergency Operations Planning*[10] standard).

Incident management system (IMS) a more fully integrated approach

The National Infrastructure Protection Plan (NIPP) Energy Sector Specific Plan (2010) states as a goal the need to achieve *"comprehensive emergency, disaster, and continuity of business planning"*[11].

Severe incident response can be managed with an incident management system (IMS) to *"direct, control, and coordinate response and recovery operations."*[12]

An approach endorsed by Congress[13] and the U.S. Department of Homeland Security[14] is contained in the National Fire Prevention Association (NFPA) Standard 1600 (Disaster/Emergency Management and Business Continuity Programs); quoted in relevant part:

"..An IMS is designed to enable effective and efficient domestic incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure..."

An IMS creates a response structure that can respond to dynamic conditions associated with severe incidents. It represents a doctrine and set of principles to organize response activities and capabilities.

Summary

Cyber-centric response activities can be integrated within an IMS approach to guide the creation of a holistic capability that can respond to severe incidents. NFPA 1600 may provide private and public operators with the guidance they need to integrate cyber-response plans into a holistic response framework.

About the author: Dave Sweigert is a Certified Information Systems Security Professional, Certified Information Systems Auditor, Project Management Professional and holds Master's degrees in Information Security and Project Management. He is a practitioner of IMS principles in his role as a volunteer Emergency Medical Technician and has attended more than 500 hours in IMS related training. He specializes in assisting organizations in institutionalizing NFPA 1600 into their cyber response plans.

[10] http://www.nerc.com/files/EOP-001-0_1b.pdf
[11] 2010 Energy Sector-Specific Plan, Page 8
[12] National Fire Protection Standard 1600, Standard on Disaster/Emergency Management and Business Continuity Programs.
[13] Intelligence Reform and Terrorism Prevention Act of 2004
[14] June 2010, DHS Secretary Napolitano formally adopts NFPA 1600 as a standard.

Expanding the role of National Guard Cyber Units to support disaster response and recovery and make a Cyber Militia a reality

January 2014

Author: Dave Sweigert, M.Sci., CISSP, CISA, PMP

ABSTRACT

Private organizations would be well advised to be aware of the involvement of National Guard cyber warfare units in responding to attacks on critical infrastructure. Increased interaction with Guard units may be appropriate for entities concerned with community-wide cyber resiliency.

Background

This year the passage of the National Defense Authorization Act (NDAA) by the U.S. Congress (used to supply the Pentagon with another year's budget) came with cybersecurity strings attached – the requirement for a comprehensive domestic cyber warfare assessment of how the National Guard would support defensive cyber warfare operations and support missions of the U.S. Department of Homeland Security.

In sum, there is likely to be a new cybersecurity player in the Critical Infrastructure – Key Resources (CIKR) arena, the National Guard.

Is this the creation of a Cyber Militia?

Cyber Militias: these are non-state sponsored collections of volunteers that can act in a militant offensive and defensive manner in cyber space. These groups can be loosely organized and operate with technical know-how to accomplish political objectives. The Chinese Eagle Union Hacker Group is one example of a "Cyber Militia".

Attacks launched by such groups that breach network cybersecurity are classified as "cyber warfare" by the Pentagon. Doomsday scenarios predict everything from massive failures of the power grid to the destruction of medical data as a consequence of an act of cyber war by such groups, creating "cyber anxiety".

Many observers have suggested that the language of the 2014 NDAA is a Dr. Strangelovian attempt to "close the cyber militia gap" and keep up with the creation of such militias in Russia, Iran, and North Korea.

Cyber Warfare: Both the National Guard Bureau (NGB) and the National Governor's Association (NGA) have openly endorsed the idea of Guard units engaged in civilian defensive cyber warfare operations.

Domestic Cyber Missions

Until now, the number of Guard units involved in civilian cybersecurity events could be counted with one hand. Examples:

Prior to the 2010 Winter Olympics the network supporting Washington State's Division of Motor Vehicles (DMV) was assessed by a Guard cyber warfare unit. Networks supporting the 2012 Presidential Inauguration were protected by such units and State networks supporting Emergency Management (E.M.) activities have also been accessed by these groups.

Such activities fall within the **National Prevention Framework** "cybersecurity" category as a **PROTECTION** capability.

With the desire of Congress to "close the gap" the scope of such support by Guard units in domestic cyber missions could be expanding. Cascading consequences created by a cyber event are addressed within the **National Response Framework** as a **RESPONSE** and **RECOVERY** activity.

State Governors could certainly activate such units during man-made cyber disasters and to support response and recovery operations in natural disasters, as well as provide support to the U.S. Department of Homeland Security missions. However, only a handful of such states have these elite cyber warfare units.

Integration with the Whole Community Concept

The Whole Community Approach to Preparedness promoted by Presidential Policy Directive 8 (**PPD-8**: National Preparedness) is a comprehensive and integrated approach to community preparedness for disasters – to include man made cyber events and their cascading consequences.

The increased interaction of public safety agencies and private entities with these National Guard cyber units in support of **PPD-8** should be addressed by the Pentagon. Alignment of Guard cyber capabilities to jointly respond with other Whole Community partners in a realistic approach to a CIKR cyber event (and the associated potential downstream effects on public utilities, medical facilities, transportation arteries, etc.) should be planned for.

Joint planning would help define how these Guard units could more effectively interface with other response agencies during cyber events and disasters. This would give Congress the Cyber Militia capability they are searching.

About the author: Dave Sweigert holds certifications as a Certified Information Systems Security Professional, Certified Information Systems Auditor, and Project Management Professional. He has earned Master's degrees in Information Security and Project Management. An Air Force veteran, he is a practitioner of cybersecurity, incident management and CIKR protection. He has consulted to Kaiser Permanente, J2 Global, NASA and the U.S. Army.

How to take down the 911 call center
-- or --
The integration of ESF 18 with NFPA 1221, Chapter 13

October 10, 2015

Author: Dave Sweigert, M.Sci., CISA, CISSP, HCISPP, PMP, SEC+

ABSTRACT

HYPOTHESIS: The next Boston Marathon style attack will be a blended operation that will include attacks on telecommunications infrastructure, to include Public Safety Answering Points (PSAPs) and public safety telecommunication services.

ASSUMPTIONS: That public safety PSAP operators may have become narrow-minded about the security of their organizations and the resolve of their adversaries.

BACKGROUND

The sophistication of cyber attacks on public safety facilities has been increasing at an alarming rate. Recent examples include:

James Boyd DDoS Attack. A Distributed Denial of Service (DDoS) attack on the City of Albuquerque (New Mexico) Police Department web-site -- coordinated with a display of civil unrest -- following the office involved shooting of a homeless man named James Boyd.

Confiscation of Michael Brown Dispatch Tapes. Following the Michael Brown shooting in Ferguson (Missouri) the "black hat" group Anonymous claimed it was able to seize the 911 emergency response tapes from the PSAP center via a penetration attack.

These attacks demonstrate that the era of general annoyance and nuisance attacks is yielding to sophisticated penetration attacks on infrastructure by cyber adversaries that are coordinating such attacks with other activities.

These attacks should serve as a wake-up call that more blended and coordinated attacks are yet to come. The Fire Service would be well served to recall that one reason for the high death toll (343) on the day of the World Trade Center (WTC) attacks was the technical communications issues with fire department radios on 9/11/2001.

Therefore, coordinated attacks that disrupt communications channels (whether 911 intake or public safety communications) can result in loss of life and property damage and should be taken seriously.

To this end, the National Fire Protection Association (NFPA) has promulgated standard 1221, "*Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*". A new effort seeks to formalize Chapter 13 into the 1221 standard, entitled "*Data Security Plan*".

In sum, the proposed Chapter 13 represents a first-step for PSAP operators to develop cyber hygiene for their organizations. It is a good first step.

However, like many other compliance driven frameworks (see Health Insurance Portability and Accountability Act (HIPAA) Security Rule) there is the temptation to treat a 1221 Data Security Plan as a check-box compliance item.

Paper-driven compliance is now obsolete

Most industries that have had a decade or more experience with compliance frameworks (like HIPAA and the Critical Infrastructure Protection (CIP) standard for the electrical power grid industry) are moving away from a paper-driven compliance framework and adopting a more active vulnerability assessment process.

Case in point. The Payment Card Industry (PCI) promulgates the Data Security Standard (DSS) for those entities processing, transmitting and storing credit card data. The PCI DSS requires quarterly vulnerability assessments and yearly penetration tests of the core infrastructure processing credit card data.

In contrast, 1221 Chapter 13 requires: a Data Security Plan composed of a Policy Statement, Procedures for Security, Assignment of Roles, Identification of Training Requirements, Security Related Training Records, etc. This is a commendable first step; but, may be "too little -- too late".

Emergency Support Function no. 18

Simultaneous with the development of 1221 Chapter 13 is the slow development of ESF no. 18 -- Cyber Security -- primarily occurring in the State of California. There have been initial exploratory meetings and preliminary task force gatherings to promote the development of ESF no. 18 -- Cyber Security.

There will continue to be a culture clash between those individuals that actively support the Information Technology (I.T.) core infrastructure of a public safety organization and those first responders that are primarily operations focused. This will be the Achilles heel that cyber adversaries will exploit to cause loss of life and property damage during a blended attack.

Now is the time to use the aegis of ESF no. 18 as an augmentation to efforts associated with NFPA 1221, Chapter 13 and bring greater awareness to the cyber threat.

Integration of cyber personnel into the Incident Command System (ICS) must begin soon, and ESF no. 18 offers the appropriate framework. Cyber experts can be classified as "Technical Specialists" under the ICS structure and can work within the Communications Unit Leader (COML) function.

Realistic exercise planning should include the loss of cyber assets due to an adversary attack and promote the interaction of cyber security experts with operations personnel.

Reconnaissance and Footprinting

Cyber adversaries are already "footprinting" PSAP centers. Open Source Intelligence (OSINT) sources are used to collect data from blogs, job boards, social media, vendor press announcements public hearings, etc. This information is being analyzed to identify the Internet and networking "footprint" of the organization.

For instance, a treasure trove of information about a PSAP facility can be obtained from the look-up services for the Domain Name Service (DNS). Lookup services provide physical addresses of facilities, contact names of key personnel, e-mail addresses, and Internet protocol (I.P.) addresses of servers and devices on the I.T. core infrastructure.

The Operating Systems (O/S) of web-facing servers are being identified using widely available tools. Once the O/S is identified, it is compared with published lists of known vulnerabilities to identify possible vulnerabilities that can be exploited with malicious code.

Enumeration and Scanning

Cyber adversaries are developing a comprehensive network map of the PSAP facility. Servers and workstations are being identified -- again, through the use of widely available tools. Cyber information probes are easily launched to circumvent Intrusion Detection Systems (IDS) and Host-based Intrusion Detections Systems (HIDS).

PSAP servers can be easily identified. Software patches released by Computer-Aided Dispatch (CAD) vendors can be collected. Attacks can be fashioned that exploit recent patches to CAD software on known servers.

In short, it is not a question of "if" a cyber attack with hit a PSAP; but, "when".

About the author: Dave Sweigert is an Emergency Medical Technician (EMT) who holds several cyber security industry certifications. An Air Force veteran, he is also an expert in auxiliary communications techniques used in disaster response. He holds Masters degrees in Information Security and Project Management.

The application of racketeering and wire fraud laws

to combat CrowdStalking hoax news sites

July 2017

Author:

Dave Sweigert, M.Sci.
Non-attorney engaged in scholarly cyber-legal research

ABSTRACT

Racketeering laws can be used to suppress CrowdStalking cyber harassment, one of the favorite operational vectors relied upon to distribute cognitive threats that are based upon deception. Hoax news sites use these techniques to attack critical infrastructure operators, federal employees, and infrastructure security advisors to create chaos in critical sectors.

The weaponization of information[1]

Blended cyber-attacks that combine assaults on (1) technical security controls, and (2) cognitive integrity may represent the most dangerous (and most misunderstood) threat on the landscape.

Cognitive integrity may be a new term for the reader. To explain, imagine the mental state of a senior C-level executive that receives a targeted spear phishing e-mail message that appears to be urgent and from the Chief Executive Officer (CEO). Cognitive integrity has been broken with the sense of urgency. The subordinate unwittingly follows orders of the hoax message and connects to a honeypot web-site where money transfer passwords can be captured. Within minutes, millions of dollars in unauthorized money wire transfers are executed with stolen password credentials.

Stalking gangs and cognitive hackers

Social media stalkers can combine information about hobbies, professional associations, fraternal organizations, etc. to craft deceptive and false messages for the purpose of supporting cyber intrusions and social engineering.

In the previous example, random bites of information are coalesced into a modern cyber weapon – the cognitive threat.

Cyber stalking gangs, encouraged by financial gain, have begun experimenting with CrowdStalking as a valid attack vector. Armies of social media vandals, well trained in areas like reputational destruction, are guided by paid social media personalities to attack targets.

CrowdStalking has turned into a type of sport or social media scavenger hunt. LiveStream technology has enabled a mass group think (mob) approach.

[1] See The Weaponization of Information: The Need for Cognitive Security, By Rand Waltzman

Suppression of the cognitive threat

Critical infrastructure (C.I.) operators should take these cognitive threats seriously. Losses in the millions of dollars can result from these cognitive attacks.

The closure of the Port of Charleston by a dirty bomb hoax is the latest example.

Legal remedies to thwart such deceptive attacks should be explored. Examples made of CrowdStalking entrepreneurs, facing serious legal consequences from their actions, can only help build a preventative deterrent to such menacing attacks.

The use of the patch-work of state and federal racketeering and wire fraud laws as a deterrent is a developing area of litigation.

In general, to establish a baseline for racketeering jurisdiction a plaintiff must demonstrate the defendant's:

1. use of either mail or wire
2. for a scheme to defraud
3. involving a material deception
4. with the intent to deprive another of
5. either property or honest services.[2]

YouTube provides hoax news operators and entrepreneurs advertiser revenue via monetization payments for videos without regard to content value.

The YouTube deception merchants are highly motivated (see the vicious cycle) to receive more revenue by broadcasting increasingly more deceptive falsehoods.

While masquerading as "news sites" and "Internet investigators", these Internet hoaxers and hatemongers deprive the general public (and their subscribers) of the expectation of honest services with their distorted "news articles".

The vicious cycle of hoax news sites

YouTube revenue is increased by viewer traffic, which is then sustained by sensationalized deception in a vicious cycle. This cycle drives increasingly more bizarre claims about individuals and institutions. Thus, revenue intake is based upon the consumption of falsehoods and misrepresentations by naïve subscribers that expect honest services and instead receive deception.

Profiting from the destruction of an individual's career or institution's reputation by trafficking in falsehoods is a popular tactic of these hoax channel operators.

CrowdStalking personalities manipulate followers (subscribers) with promises of "exposing" a target. This creates the necessary dramatic backdrop to have followers engage in spreading a deceptive narrative.

Reputational shamming and destruction may provide the needed damages to state a racketeering claim (consult with a licensed attorney). Properly classifying such activities as cyber-stalking under cognizant state law may help the judiciary understand the significance of these unlawful acts.

[2] Mail and Wire Fraud: A Brief Overview of Federal Criminal Law by Charles Doyle, Senior Specialist in American Public Law

The deception entrepreneurs

Nathan Stolpman (38) of San Luis Obispo, California, appears to represent the new era of the hoax news site entrepreneur. Stolpman seemingly holds a notorious reputation of using many of the tactics described above. Stolpman operates three YouTube channels (LIFT THE VEIL, LIFT THE VEIL TOO, and LIFT THE VEIL LIVE) as they are all in apparent various stages of "warnings" and "community strikes" (deactivation).

YouTube personality Jesse Spottswood Moorefield of Knoxville, Tennessee, operates the channel "JESSE SPOTS". Moorefield allegedly distributed videos claiming a federal employee of the U.S. National Institute of Standards and Technology (N.I.S.T.) was deeply connected with the author, as both shared the same surname. The N.I.S.T. employee was accused by Moorefield of being an integral part of a transhumanist underground that was pushing an agenda to replace mankind by 2030 with robots. All this deception was directed at a mere secretary and office coordinator, which included the display of her office symbol, telephone, home community, relatives, etc.

Stolpman and Moorefield act as associates-in-fact by coordinating their "news events" and alleged attacks on their victims.

Like Stolpman, Moorefield received several notifications (cease and desist) to halt the dissemination of falsehoods.

Enough is Enough

C.I. operators would be wise to discuss the scenarios described above with the corporate risk officer and legal counsel in the context of blended cyber-attacks.

A leaning forward legal strategy may include the consideration of claims for injunctive relief when hoax news sites and CrowdStalkers attack an institution's reputation, an individual employee or executive.

National Organization for Women, Inc. v. Scheidler, 114 S.Ct. 798 (1994); (anti-abortion protestors) is instructive on this point; quoting in relevant part:

> "We are persuaded instead that the text of the RICO[3] statute, understood in the proper light, itself authorizes private parties to seek injunctive relief."

State cyber-stalking laws should be consulted to establish a predicate criminal act as the underpinning for a potential federal racketeering claim (see Penal Code 646.9 in California or Maryland Annotated Criminal Law § 3-801).

About the author: Dave Sweigert became the target of crowdstalkers shortly after his estranged brother (George Webb Sweigert) was linked to the Port of Charleston dirty bomb hoax on 6/14/17. The author's background in computer security was seized upon as "proof" that he was an agent for government surveillance and espionage against YouTube "truth tellers" like Stolpman and Moorefield.

[3] RICO = Racketeering Influenced and Corrupt Organizations.

(EXHIBIT E)

From: **Jason Goodman** truth@crowdsourcethetruth.org
Subject: YouTube copyright complait
Date: August 21, 2020 at 11:38 AM
To: xxxsharp@xxxxxxx
Cc: Camxxx@

JG

Mr. Sharp,

I have just received notice that you have filed a copyright complaint with YouTube concerning a parody image that appeared in one of our videos. The image in question is a PARODY of the Emmy award statute and as such, you have no legitimate claim of copyright infringement. I am writing to request that you withdraw the copyright complaint immediately as it is having a direct impact on my business that may result in money damages.

Parody relies on the style of the original work and is closely imitated for comic effect and to provide criticism and commentary. This use is 1st amendment protected free speech and is also protected under Section 107 of the Copyright Act which provides for fair use under these specific circumstances. The statue is NOT depicted in its original form holding the Emmy globe but rather has been modified in a transformative way. It is shown holding a representation of a coronavirus particle and this is the essence of the comical criticism and commentary which requires the close imitation of the original for its parody effect. Parody is SPECIFICALLY protected under the digital millennium copyright act, the very same act that protects YouTube from lawsuits from third parties.

Rather than relying on further legal action, I would like to resolve this with you and I am open to discussing options that could include removing the image, the video or other remedies. What is the best way for me to reach you or your legal counsel regarding this matter?

Jason Goodman
323-744-7594

(EXHIBIT F)

Jason Goodman

Dec 22, 2022 · 3 min read · Listen

THE TWITTER COUP Part 1

Twitter's former Government Liaison Adam Sharp has stars in his eyes as he stares longingly at President Barack Obama during the Twitter Townhall @thewhitehouse July 6, 2011

Preliminary Statement

Over the past four years, U.S. District Court Judge Valerie Caproni has presided over three cases in which the author was a litigant.

(Case 1:18-cv-08653-VEC-SDA, Case 1:20-cv-07269-VEC-OTW, Case 1:21-cv-10627-VEC)

In two of the cases, the author was opposed by Adam Sharp. Facts surrounding an alleged relationship between Caproni and Sharp were unknown prior to researching and writing this article in December 2022. A motion to disqualify Caproni was denied on January 10, 2022 (Case 1:21-cv-10627-VEC Document 17).

Recusal is warranted in cases where, "a reasonable person, knowing all the facts would have doubts about the judge's ability to be impartial in the case." Judges may also recuse themselves to avoid the appearance of conflicts of interest.

The Fundamental Transformation of America

Elon Musk's "Twitter Files" reveal a deeply troubling, previously hidden relationship between federal law enforcement and private sector social media companies, but an important question remains unanswered. Who could have executed such a vast government infiltration of private industry and how could they overcome the technical and legal hurdles? As implausible as it seems, this all occurred in plain sight right under our noses over the past two decades.

Evidence in the public domain is likely to prove that former President Barack Obama, former FBI General Counsel Valerie Caproni, and Twitter's former Government Liaison Adam Sharp, were the three most important conspirators at the outset. It appears they worked together and with others to launch one of the most sinister and sophisticated crimes in our nation's history.

From Weatherman to U.S. President — The Rise of Barack Obama

Just after his historic Presidential win, the New York Times ran a story about "How Obama Tapped Into Social Networks' Power". Journalist David Carr wrote, "In February 2007, a friend called Marc Andreessen, a founder of Netscape and a board member of Facebook and asked if he wanted to meet with a man with an idea that sounded preposterous on its face." Carr never reveals the identity of Andreessen's friend but goes on to depict Obama as the genius behind a grass roots campaign facilitated by emerging technology.

In 2015, long after Ayers and Dohrn helped the obscure Illinois State Senator rise to international prominence, President Obama held a technology summit at Stanford University. After delivering remarks on the future of technology and industry, Obama signed Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing. In it, the President commanded that, "private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible." Stanford students in attendance were probably unaware, but this order codified long standing FBI demands to supersede the fourth amendment and investigate anyone they wanted. This paved the way for the Neo-fascism now being exposed in the ongoing releases of the "Twitter Files".

Making good on his campaign promise, Obama ensured that America would be fundamentally transformed from a Constitutional Republic into a Neo-fascist Technocratic Autocracy. This new authority would be enforced by a digitally enabled Super-Stasi made up of FBI InfraGard members, (https://www.infragard.org/) and other contractors including hundreds, perhaps even thousands of ordinary citizens patrolling on-line as America's Secret Police.

Such an Orwellian overthrow would be calculated to happen without anyone noticing until it was too late. The merger of government and corporate technological power enabled a class of politically aligned bureaucratic elites to maintain control by monitoring and stifling opposition rather than allowing open debate in a free marketplace of ideas. These traitors have trampled the Constitution and destroyed the most fundamental aspect of American greatness.

Part two of this series will explore Congressional allegations of criminal malfeasance within the FBI.

Twitter FBI Obama Corruption Elon Musk

Jason Goodman

Dec 22, 2022 · 2 min read · Listen

THE TWITTER COUP Part 2

Accusations of Criminal Malfeasance in the FBI General Counsel's Office

On April 14, 2010, the House Judiciary Subcommittee held a hearing on the Inspector General's "Report on the FBI's Use of Exigent Letters and Other Informal Requests for Telephone Records". Committee Chair John Conyers (D-Mich.) issued a harsh rebuke of FBI General Counsel Valerie Caproni, when he said, "Today's hearing showed that the FBI broke the law on telephone records privacy and the General Counsel's Office, headed by Valerie Caproni, sanctioned it and must face consequences."

Conyers went on to say he was "outraged" that the FBI Office of the General Counsel had invented exigent letters apparently out of whole cloth, "It's not in the Patriot Act. It never has been. And its use, perhaps coincidentally, began in the same month that Ms. Valerie Caproni began her work as general counsel."

Given the most recent revelations of Elon Musk's "Twitter Files" concerning the FBI, Conyers' closing statement in a letter to then FBI director Mueller is eerily prescient, "I'm extremely disappointed that every time Congress has tried to plug potential civil rights and civil liberties violations in our counterterrorism activities, the FBI seems to have figured out a way to get around it."

Chairman Conyers implored Mueller to take action and fire the responsible parties in Caproni's Office. No records of any action in response could be located and the press release has been removed from the House Judiciary web page.

Rather than face any consequences for her actions, Caproni would leave the FBI to join Northrup Grumman as Deputy General Counsel in 2011. She was nominated for a District Court Judge position in the Southern District of New York by Barack Obama in 2012.

During the course of her contentious Senate confirmation, Ranking Member of the Judiciary Committee Chuck Grassley sent a letter to the Dept. of Justice Office of the Inspector General. The letter detailed Senator Grassley's concerns about undue resistance to the committee's requests for documents and transcripts related to Caproni's ongoing constitutional abuses including repeated inappropriate use of National Security Letters and the even more urgent "exigent letters" throughout her tenure. The Grassley letter describes a culture of autocracy at the FBI that obstructed oversight, ignored the law and operated with impunity.

Valerie Caproni was confirmed by the Senate in 2013 and still serves as a U.S. District Court Judge for the Southern District of New York where she continues her abuse of citizens' constitutional rights to this day.

Part three will discuss how technical and legal barriers were overcome in the effort to destroy Americans' constitutional protections.

FBI Twitter Valerie Caproni Corruption Congress

Jason Goodman

Dec 22, 2022 · 4 min read · Listen

THE TWITTER COUP Part 3

President George W. Bush and a gaggle of neocon cronies delight in laying the groundwork for the destruction of the U.S. Constitution

Overcoming Legal Hurdles Takes a Village

The groundwork was laid by the George W. Bush Administration. In the wake of the national trauma of 9/11, the Patriot Act was passed under the guise of increased security. This unconstitutional statute called for the creation of the National Cyber Investigative Joint Task Force, an interagency intelligence sharing organization led by the FBI. It also granted federal law enforcement new tools in their self-declared "war on terror". For the first time since the signing of the Bill of Rights, federal agents were granted unilateral authority to surveil any person they deemed a national security threat without first establishing probable cause or providing any evidence to a judge. Due process was bypassed, the need for warrants ignored, and newly created National Security Letters decimated the Fourth Amendment.

No longer were We the People "secure in our persons, houses, papers, and effects, against unreasonable searches and seizures". The FBI and other Federal agencies could simply send a National Security Letter to your phone company or internet provider seeking any information associated with any account for any reason. Although National Security Letters do not have the same legal force and effect as Court Orders or properly issued search warrants, the practical impact is virtually identical with an historical record nearing 100% compliance by providers.

During her tenure as general counsel at the FBI, Valerie Caproni coined the phrase "Going Dark". The term purported to describe an increasing proliferation of digital communications technologies and a widening gap in law enforcement's ability to penetrate those technologies in the due course of criminal investigations. Things like end-to-end encryption and automatically decimated chat logs had investigators in the dark according to Caproni.

The FBI's proposed solution was to create new legislation granting agencies unfettered access to all digital communications in real time. Setting aside the unrealistic network bandwidth and storage requirements of such a concept, the idea was controversial to say the least. Caproni and the FBI aimed to compel all technology companies to modify their products with "back doors" that would bypass primary security measures and allow federal investigators instant and full access to any account upon receipt of a National Security Letter.

Caproni would come under fire throughout her career for gross abuses of the process including the arbitrary creation of so called "exigent letters" which have no statutory

basis in the Patriot Act and the reliance on false statements to open alleged counterintelligence investigations.

https://www.c-span.org/video/?197219-1/fbi-national-security-letters

https://www.grassley.senate.gov/imo/media/doc/judiciary/upload/Caproni-03-19-13-letter-to-OIG-requesting-information.pdf

https://www.techdirt.com/2013/09/09/former-fbi-lawyer-who-oversaw-years-fourth-amendment-violations-agency-nominated-federal-judge-seat/

https://www.washingtonpost.com/world/national-security/former-fbi-official-questioned-on-abuse-of-intelligence-gathering-tools/2013/02/04/b228c4dc-6eef-11e2-aa58-243de81040ba_story.html

Caproni and her successors Andrew Weissman and James Baker went as far as suggesting modifications that amounted to hobbling the most sophisticated products available. These products' creators admonished FBI luddites and articulated how the changes would dramatically weaken security and expose all users to data theft and hacking. Despite a fundamental lack of subject matter knowledge, for years the FBI continued to make demands that industry experts argued would pose too great a risk for everyone should they be compelled to comply.

A Decade of "Going Dark"

Nearly eight years after Valerie Caproni delivered an address at Lewis & Clark Law School on "Crimes, War Crimes, and the War on Terror", the New York Times reported, "Obama Won't Seek Access to Encrypted User Data". Perhaps this was true of encrypted data, but perhaps this was just a lawyerly way of talking around a new cooperative plan to intercept data at the source, before it was encrypted or after it had been decrypted. Going back as far as 2005, Caproni had made the FBI's position on "Going Dark" extremely clear, it was a top priority. The persistence with which the FBI pursued this agenda cannot be overstated, nor can the public resistance to it.

Would secretly planting FBI operatives directly inside Twitter allow agents to address management's "Going Dark" concerns without the need to crack encryption keys or reveal their efforts to the public? Could such a cozy relationship indicate that Twitter

had agreed to implement the long-sought FBI back door without informing unsuspecting users? Twitter's new CEO has revealed emails indicating reimbursements to Twitter from the FBI for the fulfilment of requests related to investigations. While Twitter's CEO may have incorrectly characterized the nature and purpose of the payments, it is not denied that the payments were made.

Was Twitter motivated to comply with FBI investigation requests by law or by financial incentives? Did the FBI need warrants to investigate, penetrate or terminate the private Twitter accounts of U.S. citizens? These and other questions remain open. Many may ask, would the FBI do something illegal? Would they take action even if it had no basis in law? House and Senate oversight of the FBI General Counsel's Office and the Inspector General's report on the matter indicate they were in a regular practice of doing exactly that.

Part four will reveal how the U.S. Government essentially became one with private industry when it infiltrated Twitter.

Twitter Elon Musk FBI Patriot Act Valerie Caproni

Jason Goodman
Dec 22, 2022 · 4 min read · Listen

THE TWITTER COUP Part 4

President Barack Obama and Twitter CEO Jack Dorsey at the Whitehouse Twitter Town Hall July 6, 2011

The Marriage of the U.S. Government and Social Media

Although Barack Obama does not consider himself a luddite, during a 2022 address at the Stanford Internet Observatory he admitted he has to ask his "daughters how to work basic functions" on his phone. Even fifteen years after joining Twitter, Barack Obama's background, experience and technological profile is inconsistent with that of

someone who could have foreseen the impact social media would have on politics all the way back in 2007.

It is impossible to understand the U.S. Government's infiltration into Twitter without exploring the role of the man who is most likely to have presided over this unholy union. Today, he is the President and CEO of the National Academy of Television Arts and Sciences ("NATAS"), an obscure individual named Adam Sharp. Before handing out EMMY awards, Sharp joined Twitter in its pre-IPO days, early in November of 2010. Hot topics in DC at that time included regulation of social media firms. It was quietly coming out that many had hired lobbyists to get in front of the issue. Just prior to Sharp joining Twitter, in October of 2010, the LA Times ran an op-ed reporting "Facebook lobbies California on online privacy act (but shhh — don't tell anyone).

Evidence indicates Sharp's interest in Twitter began long before he was hired there. While serving as an Executive Producer for C-SPAN in 2009, Sharp launched a public affairs database that included "Twitter and Facebook API integration". API stands for application programming interface and describes a set of software tools provided to developers to enable customization and integration with other products. Sharp's utilization of Twitter's development API is an indication that he was very familiar with the inner workings and unrealized potential of Twitter at least by 2009, likely prior.

Sharp's online resume fails to discuss Valerie Caproni's appearance on C-SPAN3 in June of 2009 during the time he was the Executive Producer and managed primetime programming. It is difficult to imagine that the Executive Producer would not interact at all with such an important FBI guest. At very least, as programming manager, Sharp would be aware of the content of the broadcast in which Caproni articulated the FBI's goals to penetrate online communications. It remains unknown if any interaction occurred between Sharp and Caproni. Even in the event that there was none, Sharp was very likely aware of the FBI's concerns about "Going Dark" as long ago as 2009.

While at Twitter, Sharp made incredible inroads both for the company and the U.S. Government. https://www.cnn.com/2015/02/03/politics/twitter-washington-office

Throughout his time at Twitter, Sharp separately owned and operated Sharp Political Consulting, LLC. Sharp incorporated this firm in April of 2007. This is notably close in time proximity to the March 5, 2007 creation of the @barackobama Twitter account

cited in the Atlantic Magazine article, "You're Not Really Following @BarackObama on Twitter".

Creation of Obama's now famous Twitter account is especially notable because Twitter was virtually unknown in 2007. Jack Dorsey had published the world's first Tweet less than one year prior on March 21, 2006. Obama was not only one of the first politicians to join Twitter, but he was also among the first of all users. Technology moguls including current Twitter CEO Elon Musk, and former Microsoft CEO Bill Gates would not join until years later in June 2009. No other person fits the profile or was in the position to put Barack Obama and Twitter together in the way Adam Sharp clearly was.

Journalist Phillip Bump told Atlantic Magazine readers that Obama's "Twitter account was created by a staffer on March 5, 2007, two months before he formally announced his Presidential candidacy." The Senate staffer has never been identified, but Sharp was serving as Deputy Chief of Staff for Senator Mary L. Landrieu at the time. An election postmortem from the New York Times citing Obama's genius in leveraging social media declared an anonymous "friend" brought Marc Andreessen to the Obama campaign. Could both of these anonymous King Makers be Sharp? The answer remains a mystery, but it is likely 'yes'.

Even after Sharp became Twitter's official Government Liaison, Sharp Political Consulting, LLC remained active and engaged in matters that do not seem to have clear connections to Twitter.

Sharp Political Consulting made over $50,000 in political contributions to Democrat candidates in 2014.

In January 2016, pollsters calculated a 71% likelihood of a Hillary Clinton presidential win. For reasons that are unclear, Sharp voluntarily dissolved Sharp Political Consulting, LLC on January 29, 2016. In December 2016, less than one year later and precisely one month after Donald Trump's largely unexpected victory over Clinton, Sharp abruptly left his beloved Twitter and promptly formed SharpThings, LLC, just one week after the press release announcing his departure. Sharp would spend a lot of time lecturing about Disinformation in various public speaking engagements from 2016 through 2018 and then during his tenure as CEO of NATAS beginning in 2018. Was

Sharp's departure motivated by an urgent need to step up *la Résistance* to Donald Trump?

Part five will bring the story up to today and connect the suspected conspirators to the events being exposed in The TWITTER FILES.

Obama Jack Dorsey Twitter FBI Elon Musk

Jason Goodman

Dec 22, 2022 · 3 min read · Listen

THE TWITTER COUP Part 5

President Barack Obama, Twitter Head of News, Politics and Elections Adam Sharp, Twitter General Counsel Alexander Macgillivray and other staff members celebrate their success at the Whitehouse on July 6, 2011

Operational Deployment of FBI–Twitter

For more than a decade, FBI leadership was acutely focused on a "Going Dark" public relations campaign. James Comey and Christopher Wray each spoke about it throughout their respective tenures as FBI Director.

But it was Valerie Caproni's disciples in the FBI General Counsel's office that finally made the plans operational. Her direct successor Andrew Weissman led the Mueller Investigation into Russian Collusion with the Donald Trump Presidential Campaign. This investigation was marred by the abuse of the secret FISA Court process and was distinctly categorized by Mueller's team as a Counterintelligence investigation rather than a criminal investigation. This distinction allowed investigators to access the unconstitutional and disputed powers imbued upon the FBI by Caproni. Ultimately, no evidence was found to substantiate the Mueller accusations.

Because the mere suggestion of Russian interference with a U.S. Presidential election represents a national security threat, the accusation alone absent evidence, was legally sufficient to open an investigation under the Patriot Act. This would have allowed Andrew Weissmann to use National Security Letters to merely allege that Trump represented a national security threat and initiate the years long and highly disruptive probe. This is perhaps the clearest example of naked abuse of the Patriot Act since its inception and provides good grounds for its termination.

Weissmann's successor James Baker. Director Comey appointed Baker General Counsel of the FBI on January 15, 2014. Baker was reassigned by Wray in 2017 and then resigned amid accusations that he leaked classified documents related to the Mueller investigation of Trump.

Senior Fellow in Governance Studies at the Brookings Institution, Benjamin Wittes was the likely recipient of the leak. Wittes is the editor of Lawfare, an online publication of the Brookings Institution that James Comey told an audience he reads every day. Wittes has claimed to be among James Comey's closest friends. Baker would transition to Brookings and Lawfare after departing the FBI and prior to becoming Twitter's Deputy General Counsel. The Brookings Institution is a non-profit think tank and a potential incubator for domestic coup d'etats, perhaps along the lines of what was done with Twitter. Baker appeared on MSNBC as recently as 2019 restating unconstitutional FBI demands to access everyone's data at any time.

FBI All in at Twitter

On or around May 28, 2020, a new Twitter policy began adding warnings to "fact check" users' Tweets. After warnings were applied to Tweets sent from @realDonaldTrump, the President issued executive order 13925 titled "Preventing Online Censorship". The order sought to curb perceived abuse of 47 USC § 230, the infamous Communications Decency Act that shields online service providers from liability even if they editorialize content that does not violate the law or civil torts. If implemented, the proposed changes threatened to expose Twitter to thousands of civil legal actions. Less than three weeks after Trump's order, former FBI General Counsel Baker joined Twitter as Deputy General Counsel. Was this a coincidence or was Baker still serving the demands of his long-time FBI colleagues? Baker had transitioned through the FBI revolving door of non-profit think tanks, including the Brookings Institution, Lawfare and the R Street Institute, following the plan articulated in Obama's 2015 Stanford inspired order.

It has now been widely reported that during Baker's time as Deputy General Counsel, Twitter suppressed a true and accurate news story published by the New York Post that likely affected the outcome of the 2020 Presidential election. Dr. Michael Shellenberger provides evidence of communications between FBI Special Agent Elvis Chan and employees of Twitter in the Twitter Files 7.

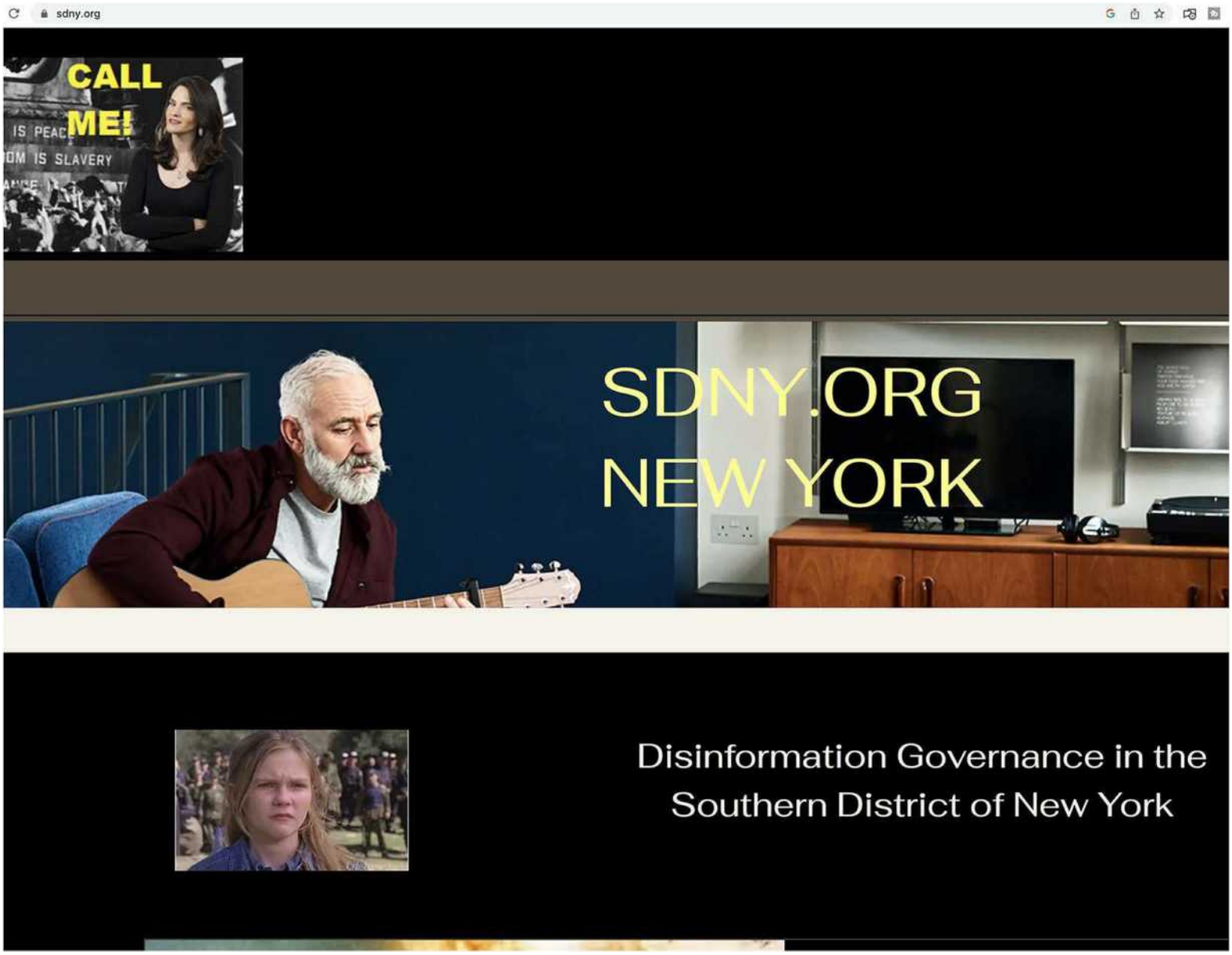
The communications indicate the FBI had foreknowledge of facts that would be asserted by the New York Post and knew them to be true, but falsely informed Twitter it was the product of a Russian "hack and leak" operation.

Now we stand at the brink of world war in Ukraine. Even stating the opinion "Joe Biden and Twitter rigged the 2020 election with the help of the FBI" is considered spreading disinformation. The FBI and CISA have determined disinformation is a national security threat. This logically could lead to the FBI investigating you if they decide something you say is false.

America has been transformed right before our eyes, and all that was needed was a pen and a phone.

Sources and Additional Information

(EXHIBIT G)


sdny.org
CALL
ME!
IS PEACE
OM IS SLAVERY
SDNY.ORG
NEW YORK
Disinformation Governance in the
Southern District of New York

(EXHIBIT H)

Thread

Centre for Information Resilience
@Cen4infoRes

We are delighted to announce disinformation expert Nina Jankowicz (@wiczipedia) has joined CIR.

Nina will help lead our efforts in countering hostile state efforts to distort the information space.

She'll also be launching the Hypatia Project 👇

info-res.org
Announcing The Hypatia Project: Combating Gendered Abuse and Disinformati...
During Kamala Harris's historic Vice-Presidential campaign, she faced a torrent of online abuse and lies that claimed she "slept her way to the top." Online ...

9:12 AM · Sep 23, 2022

30 Retweets **25** Quote Tweets **114** Likes

U.S. Department of Justice
Washington, DC 20530

Exhibit A to Registration Statement
Pursuant to the Foreign Agents Registration Act of 1938, as amended

INSTRUCTIONS. Furnish this exhibit for EACH foreign principal listed in an initial statement and for EACH additional foreign principal acquired subsequently. The filing of this document requires the payment of a filing fee as set forth in Rule (d)(1), 28 C.F.R. § 5.5(d)(1). Compliance is accomplished by filing an electronic Exhibit A form at https://www.fara.gov.

Privacy Act Statement. The filing of this document is required by the Foreign Agents Registration Act of 1938, as amended, 22 U.S.C. § 611 *et seq.*, for the purposes of registration under the Act and public disclosure. Provision of the information requested is mandatory, and failure to provide this information is subject to the penalty and enforcement provisions established in Section 8 of the Act. Every registration statement, short form registration statement, supplemental statement, exhibit, amendment, copy of informational materials or other document or information filed with the Attorney General under this Act is a public record open to public examination, inspection and copying during the posted business hours of the FARA Unit in Washington, DC. Statements are also available online at the FARA Unit's webpage: https://www.fara.gov. One copy of every such document, other than informational materials, is automatically provided to the Secretary of State pursuant to Section 6(b) of the Act, and copies of any and all documents are routinely made available to other agencies, departments and Congress pursuant to Section 6(c) of the Act. The Attorney General also transmits a semi-annual report to Congress on the administration of the Act which lists the names of all agents registered under the Act and the foreign principals they represent. This report is available to the public in print and online at: https://www.fara.gov.

Public Reporting Burden. Public reporting burden for this collection of information is estimated to average .22 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Chief, FARA Unit, Counterintelligence and Export Control Section, National Security Division, U.S. Department of Justice, Washington, DC 20530; and to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503.

1. Name of Registrant
Ms. Nina Jankowicz

2. Registration Number
7192

3. Primary Address of Registrant
1405 S Fern St #547, Arlington, VA 22202

4. Name of Foreign Principal
Centre for Information Resilience

5. Address of Foreign Principal
International House, 24 Holborn Viaduct
London, United Kingdom
UNITED KINGDOM EC1A 2BN

6. Country/Region Represented
UNITED KINGDOM

7. Indicate whether the foreign principal is one of the following:

- ☐ Government of a foreign country[1]
- ☐ Foreign political party
- ☒ Foreign or domestic organization: If either, check one of the following:
  - ☐ Partnership
  - ☒ Corporation
  - ☐ Association
  - ☐ Committee
  - ☐ Voluntary group
  - ☐ Other *(specify)* _____
- ☐ Individual-State nationality _____

8. If the foreign principal is a foreign government, state:

a) Branch or agency represented by the registrant

b) Name and title of official with whom registrant engages

1 "Government of a foreign country," as defined in Section 1(e) of the Act, includes any person or group of persons exercising sovereign de facto or de jure political jurisdiction over any country, other than the United States, or over any part of such country, and includes any subdivision of any such group and any group or agency to which such sovereign de facto or de jure authority or functions are directly or indirectly delegated. Such term shall include any faction or body of insurgents within a country assuming to exercise governmental authority whether such faction or body of insurgents has or has not been recognized by the United States.

Received by NSD/FARA Registration Unit 11/18/2022 12:02:14 PM

9. If the foreign principal is a foreign political party, state:

a) Name and title of official with whom registrant engages

b) Aim, mission or objective of foreign political party

10. If the foreign principal is not a foreign government or a foreign political party:

a) State the nature of the business or activity of this foreign principal.

Non-profit social enterprise focused on countering disinformation, documenting human rights abuses, and combating online harms against women and minorities

b) Is this foreign principal:

Supervised by a foreign government, foreign political party, or other foreign principal	Yes ☐ No ☒
Owned by a foreign government, foreign political party, or other foreign principal	Yes ☐ No ☒
Directed by a foreign government, foreign political party, or other foreign principal	Yes ☐ No ☒
Controlled by a foreign government, foreign political party, or other foreign principal	Yes ☐ No ☒
Financed by a foreign government, foreign political party, or other foreign principal	Yes ☒ No ☐
Subsidized in part by a foreign government, foreign political party, or other foreign principal	Yes ☐ No ☒

11. Explain fully all items answered "Yes" in Item 10(b).

Item 10(b) Financed: CIR is financed in part by grants from the UK Government, including the Foreign, Commonwealth, and Development Office.

12. If the foreign principal is an organization and is not owned or controlled by a foreign government, foreign political party or other foreign principal, state who owns and controls it.

CIR is a non-profit social enterprise founded and directed by a UK citizen, Adam Rutland, and a dual UK-US national, Ross Burley.

EXECUTION

In accordance with 28 U.S.C. § 1746, and subject to the penalties of 18 U.S.C. § 1001 and 22 U.S.C. § 618, the undersigned swears or affirms under penalty of perjury that he/she has read the information set forth in this statement filed pursuant to the Foreign Agents Registration Act of 1938, as amended, 22 U.S.C. § 611 *et seq.*, that he/she is familiar with the contents thereof, and that such contents are in their entirety true and accurate to the best of his/her knowledge and belief.

Date	Printed Name	Signature
11/18/2022	Nina Jankowicz	/s/Nina Jankowicz

EXECUTION

In accordance with 28 U.S.C. § 1746, and subject to the penalties of 18 U.S.C. § 1001 and 22 U.S.C. § 618, the undersigned swears or affirms under penalty of perjury that he/she has read the information set forth in this statement filed pursuant to the Foreign Agents Registration Act of 1938, as amended, 22 U.S.C. § 611 *et seq.*, that he/she is familiar with the contents thereof, and that such contents are in their entirety true and accurate to the best of his/her knowledge and belief.

Date	Printed Name	Signature
18 Nov 2022	Nina M. Jankowicz	Nina Jankowicz

U.S. Department of Justice

Washington, DC 20530

Exhibit B to Registration Statement Pursuant to the Foreign Agents Registration Act of 1938, as amended

INSTRUCTIONS. A registrant must furnish as an Exhibit B copies of each written agreement and the terms and conditions of each oral agreement with his foreign principal, including all modifications of such agreements, or, where no contract exists, a full statement of all the circumstances by reason of which the registrant is acting as an agent of a foreign principal. Compliance is accomplished by filing an electronic Exhibit B form at https://www.fara.gov.

Privacy Act Statement. The filing of this document is required for the Foreign Agents Registration Act of 1938, as amended, 22 U.S.C. § 611 *et seq.*, for the purposes of registration under the Act and public disclosure. Provision of the information requested is mandatory, and failure to provide the information is subject to the penalty and enforcement provisions established in Section 8 of the Act. Every registration statement, short form registration statement, supplemental statement, exhibit, amendment, copy of informational materials or other document or information filed with the Attorney General under this Act is a public record open to public examination, inspection and copying during the posted business hours of the FARA Unit in Washington, DC. Statements are also available online at the FARA Unit's webpage: https://www.fara.gov. One copy of every such document, other than informational materials, is automatically provided to the Secretary of State pursuant to Section 6(b) of the Act, and copies of any and all documents are routinely made available to other agencies, departments and Congress pursuant to Section 6(c) of the Act. The Attorney General also transmits a semi-annual report to Congress on the administration of the Act which lists the names of all agents registered under the Act and the foreign principals they represent. This report is available to the public in print and online at: https://www.fara.gov

Public Reporting Burden. Public reporting burden for this collection of information is estimated to average .32 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Chief, FARA Unit, Counterintelligence and Export Control Section, National Security Division, U.S. Department of Justice, Washington, DC 20530; and to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503.

1. Name of Registrant	2. Registration Number
Ms. Nina Jankowicz	7192

3. Name of Foreign Principal
Centre for Information Resilience

Check Appropriate Box:

4. ☒ The agreement between the registrant and the above-named foreign principal is a formal written contract. If this box is checked, attach a copy of the contract to this exhibit.

5. ☐ There is no formal written contract between the registrant and the foreign principal. The agreement with the above-named foreign principal has resulted from an exchange of correspondence. If this box is checked, attach a copy of all pertinent correspondence, including a copy of any initial proposal which has been adopted by reference in such correspondence.

6. ☐ The agreement or understanding between the registrant and the foreign principal is the result of neither a formal written contract nor an exchange of correspondence between the parties. If this box is checked, give a complete description below of the terms and conditions of the oral agreement or understanding, its duration, the fees and expenses, if any, to be received.

7. What is the date of the contract or agreement with the foreign principal? 09/29/2022

8. Describe fully the nature and method of performance of the above indicated agreement or understanding.

Jankowicz works regularly via online communication platforms with CIR employees based in the UK in order to further the goals of CIR.

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

9. Describe fully the activities the registrant engages in or proposes to engage in on behalf of the above foreign principal.

Jankowicz supervises research, executes business strategy, oversees the establishment of CIR's research, communicates with the media, and briefs individuals and officials on CIR's research.

10. Will the activities on behalf of the above foreign principal include political activities as defined in Section 1(o) of the Act[1].

Yes ☐ No ☒

If yes, describe all such political activities indicating, among other things, the relations, interests or policies to be influenced together with the means to be employed to achieve this purpose. The response must include, but not be limited to, activities involving lobbying, promotion, perception management, public relations, economic development, and preparation and dissemination of informational materials.

11. Prior to the date of registration[2] for this foreign principal has the registrant engaged in any registrable activities, such as political activities, for this foreign principal?

Yes ☒ No ☐

If yes, describe in full detail all such activities. The response should include, among other things, the relations, interests, and policies sought to be influenced and the means employed to achieve this purpose. If the registrant arranged, sponsored, or delivered speeches, lectures, social media, internet postings, or media broadcasts, give details as to dates, places of delivery, names of speakers, and subject matter. The response must also include, but not be limited to, activities involving lobbying, promotion, perception management, public relations, economic development, and preparation and dissemination of informational materials.

Set forth below a general description of the registrant's activities, including political activities.

Jankowicz interfaced with the media using her CIR affiliation. Those instances are below. From September 29-present, she also engaged on social media (Twitter, LinkedIn, Instagram) as a CIR principal.

Set forth below in the required detail the registrant's political activities.

Date	Contact	Method	Purpose
09/23/2022	info-res.org	Website	Announcing joining CIR, work on gender and abuse
09/29/2022	Washington Post	Print	Discuss tools to scrub personal information from internet for online safety
10/20/2022	Connecticut Public Radio	Radio	Discuss online abuse and disinformation
10/23/2022	NPR	Radio	Discuss Russian disinformation in the Ukraine war
10/31/2022	Inkstick Media	Podcast	Discuss online disinformation and abuse
11/08/2022	NPR	Radio	Discuss Russian disinformation ahead of the 2022 midterms
11/11/2022	Radio Free Asia	Print	Quote about G20 condemnation of Russia

12. During the period beginning 60 days prior to the obligation to register[3] for this foreign principal, has the registrant received from the foreign principal, or from any other source, for or in the interests of the foreign principal, any contributions, income, money, or thing of value either as compensation, or for disbursement, or otherwise?

Yes ☒ No ☐

If yes, set forth below in the required detail an account of such monies or things of value.

Date Received	From Whom	Purpose	Amount/Thing of Value
10/17/2022	CIR	Remuneration for services rendered	$ 12,115.18
11/17/2022	CIR	Remuneration for services rendered	$ 12,071.41
		Total	$ 24,186.59

13. During the period beginning 60 days prior to the obligation to register[4] for this foreign principal, has the registrant disbursed or expended monies in connection with activity on behalf of the foreign principal or transmitted monies to the foreign principal?

Yes ☐ No ☒

If yes, set forth below in the required detail and separately an account of such monies, including monies transmitted, if any.

Date	Recipient	Purpose	Amount

1 "Political activity," as defined in Section 1(o) of the Act, means any activity which the person engaging in believes will, or that the person intends to, in any way influence any agency or official of the Government of the United States or any section of the public within the United States with reference to formulating, adopting, or changing the domestic or foreign policies of the United States or with reference to the political or public interests, policies, or relations of a government of a foreign country or a foreign political party.

2,3,4 Pursuant to Section 2(a) of the Act, an agent must register within ten days of becoming an agent, and before acting as such.

EXECUTION

In accordance with 28 U.S.C. § 1746, and subject to the penalties of 18 U.S.C. § 1001 and 22 U.S.C. § 618, the undersigned swears or affirms under penalty of perjury that he/she has read the information set forth in this statement filed pursuant to the Foreign Agents Registration Act of 1938, as amended, 22 U.S.C. § 611 *et seq.*, that he/she is familiar with the contents thereof, and that such contents are in their entirety true and accurate to the best of his/her knowledge and belief.

Date	Printed Name	Signature
11/18/2022	Nina Jankowicz	/s/Nina Jankowicz

EXECUTION

In accordance with 28 U.S.C. § 1746, and subject to the penalties of 18 U.S.C. § 1001 and 22 U.S.C. § 618, the undersigned swears or affirms under penalty of perjury that he/she has read the information set forth in this statement filed pursuant to the Foreign Agents Registration Act of 1938, as amended, 22 U.S.C. § 611 *et seq.*, that he/she is familiar with the contents thereof, and that such contents are in their entirety true and accurate to the best of his/her knowledge and belief.

Date	Printed Name	Signature
18 Nov 2022	Nina M. Jankowicz	Nina Jankowicz

Sophias Strategies, LLC, c/o Nina Jankowicz, Founder.

Centre for Information Resilience
International House
24 Holborn Viaduct
London
EC1A 2 BN

Dear Nina,

- This engagement letter ("Letter of Engagement") between you, Nina Jankowicz, as the Consultant and the Centre for Information Resilience C.I.C ("CIR") together with the Terms of Reference at Annex 1, the General Terms and Conditions at Annex 2 and the Statement of Compliance at Annex 3 constitute the entire agreement between the parties whereby the Consultant will provide the services set out in the Terms of Reference. In the event of and only to the extent of any conflict between the various parts of the Agreement, the order of priority shall be as follows: (i) special conditions; (ii) Letter of Engagement, (iii) General Terms and Conditions, (iv) Terms of Reference. In respect of the General terms and Conditions these must be considered and applied at all times as an integral part of the Contract.

- "**Services**" means:

  The Consultant will work with the CIR team to undertake the tasks outlined in the Terms of Reference:

  In undertaking the Services the Consultant will be contractually responsible to CIR for the appropriateness, quality and timeliness of the work done. Day to day tasking, and the completion and agreement of deliverables will be a matter for the Consultant to handle with the nominated representative of CIR, Adam Rutland, or their nominate substitute

- **Remuneration**

  Remuneration for this contract is input based plus Reimbursable Expenses (See clause 4 below) calculated as follows:

  The day rate of £450 per day, for 12 months plus VAT/GST (if applicable) for the consultant's time properly occupied in or in connection with the Services during the Duration, agreed before the event with the Project Director and accurately recorded in a timesheet using CIR's agreed timesheet template.

  We assume a five-day working week and an eight-hour working day, unless agreed otherwise with CIR, and one day travel per overseas visit.

- **Reimbursable Expenses:**

  CIR shall reimburse the Consultant for reasonable out of pocket expenses for travel, accommodation, subsistence and incidental expenses incurred directly in the provision of the Services and agreed in advance with the Project Director, and only where supported by receipts

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

or other such written support for the expenditure. All hotel receipts, actually used air tickets and boarding passes MUST be retained and submitted along with invoices to CIR.

For clarification, CIR will reimburse the adviser for the cost of travel (economy flights, airport transfers, in-country transport), subsistence, accommodation and visas incurred by the Consultant during the provision of the Services overseas, in line with the provisions set out in CIR's HR Handbook. Originals of receipt must be retained and provided to CIR upon request. Failure to provide receipts may result in the inability of CIR to reimburse all or part of expenses incurred, or may require the company to deduct the amounts involved from a subsequent payment if absence of the receipts has prevented CIR from receiving payment from its client.

Itemised expenses must be submitted to CIR as a sub-section of the Consultant's invoice (see general terms and conditions), with receipts attached as an Annex. In the event the expense is incurred in a different currency to the currency of payment of the Remuneration (in section 3 above), the Consultant must use XE (www.xe.com) to convert the expense into the applicable currency using the rate from the date on which the expense was incurred.

- **Duration**

  It is anticipated that the Consultant will be required to carry out the Services from 5th September 2022 until 5th September 2023 or until such other later date as may be agreed in writing between the Parties. An input of 5 days per week is anticipated, as specified in the Terms of Reference.

  Either party may terminate this Letter of Engagement at any time in accordance with clause 12 of the General Terms and Conditions. CIR and the Consultant shall agree any further term giving the Consultant a minimum of 14 days notice. The General Terms and Conditions shall continue to apply to any new or extended contract agreed between CIR and the Consultant.

- **Contact details**

  "Project Director" means Adam Rutland or such person that may be named in their place by CIR

- **Additional Requirements**

- By signing this letter of engagement, the Consultant agrees to accept CIR's Consultant General Terms and Conditions as set out in Annex 2.

For an on behalf of the Centre for Information Resilience

Ross Burley 29/09/2022

I confirm that I have read, understood and agree to the terms and conditions of this agreement

Nina Jankowicz 29/09/2022

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

Annex 1 Terms of Reference: Vice President, U.S.

About the Role

The Centre for Information Resilience is a UK based, independent, non-profit social enterprise. We counter disinformation, expose human rights abuses through open source and combat online harms targeting women and minorities.

We have established ourselves as a trusted, innovative NGO among UK media and policymakers. We work frequently with UK government colleagues to help in the areas above. We are now looking for an experienced disinformation expert to raise our profile among policymakers, media and potential donors based in the United States. This is a key role in a growing organisation. You will work closely with the co-founders and will be a leadership figure – mentoring and leading more junior members of the organisation.

We require a self-starter, comfortable with taking the initiative and seizing opportunities. You will be adept at briefing senior policymakers and talking to US media organisations, both on and off the record.

You will be ambitious to build networks, with a focus on government, congress, tech and philanthropic organisations. Helping CIR to secure funding – through grants / donations will be a priority. Should you be successful, designing and building up a larger CIR team based in the US will be encouraged / supported.

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

As well as the outward facing aspects of the role, you will be a valued researcher, able to help talented researchers develop methodologies / investigations to counter disinformation. We require an outstanding communicator, able to explain complex, difficult subjects into easy to understand written and spoken language.

Specific tasks will include:

- Provide leadership in the delivery of investigations, including providing technical inputs into, and quality assurance of, research methodologies, activities and outputs – ensuring CIR research is delivered to time, budget and in line with client/CIR quality and ethical standards
- Identify and take forward business development opportunities, including developing project bids/proposals and client presentations
- Act as an ambassador for CIR on the Hill, within the Federal Government, media, among tech companies / Silicon Valley, on "K Street", and among potential philanthropic organisations. Identify and build relationships within those groups, prioritizing who you think will provide greatest impact for a) raising awareness of CIR and b) providing funding for CIR – keeping co-founders aware of activities through regular updates
- Act as a spokesperson for CIR, appearing on US media organisations, in consultation with the Head of Media / co-founders. Develop relationships with key US outlets, and advise the Head of Media on where specific investigations may land / be appropriate for partnerships

Person Specification

Essential Criteria:

- Excellent written and verbal communication skills, including the ability to translate technical terminology for lay audiences and to produce clear, concise language
- Established outstanding credentials in identifying and exposing disinformation and influence operations; a record working with governments / multilateral institutions or the media to identify or counter disinformation
- Excellent stakeholder and relationship management skills
- Significant experience with media, including experience with live broadcasts

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

- Strong research experience – able to design methodologies and lead research teams.

Management arrangements

This role will report to the Co-Founders.

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

Annex 2: General Terms and Conditions

October 2020

CENTRE FOR INFORMATION RESILIENCE

CONSULTANT GENERAL TERMS AND CONDITIONS

Interpretation of this Agreement

Any capitalised terms used but not defined herein shall have the meaning given to them in the Letter of Engagement.

IT IS AGREED between Centre for Information Resilience C.I.C. together with its affiliates, ("CIR") and the Consultant as follows:

PROVISION OF SERVICES

The Consultant agrees to provide CIR with the Services. All time spent is to be agreed before the event with the Project Director.

The Consultant confirms that the content of his/her curriculum vitae is factually correct and does not misrepresent the Consultant's suitability to carry out the Services.

The Consultant confirms that he/she has provided true and accurate information to CIR to enable CIR to carry out thorough background screening procedures on the Consultant in accordance with its own policies and any applicable Client vetting procedures and the Consultant warrants that it will inform the Project Director as soon as practicable if the Consultant becomes aware of any information during provision of the Services that could reasonably cause further background screening processes to be carried out.

The Consultant undertakes to carry out the Services to at least the minimum, standard of care and technical and professional expertise required by a reputable international management consultancy. The Consultant warrants that he/she is appropriately qualified, experienced and in a suitable physical condition to carry out the Services.

The Consultant recognises that in carrying out the Services, he/she is doing so as a representative of CIR. As such, the Consultant shall ensure that at all times he/she acts properly and professionally in performing the Services and does not do anything that could damage the reputations of CIR or the Client.

The Consultant shall be available to work at such times as are agreed between the Consultant and the Project Director, from time to time, to properly perform the Services.

The Consultant acknowledges and understands that by entering into this Agreement, any further work for CIR is not guaranteed after the Services are completed.

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

In circumstances where the Consultant is unable to continue to perform the Services, the parties may agree to appoint a suitable qualified, vetted and skilled substitute to perform the Services on the Consultant's behalf ("The Substitute"). In such circumstances, the Substitute shall be provided by the Consultant and required to enter into direct undertakings with CIR, to the same level as detailed in this Agreement, including those relating to confidentiality before any substitution of work is undertaken.

FINANCIAL ARRANGEMENTS

CIR will pay the Consultant fees and reimbursable expenses and/or per diems on the basis as set out in the Letter of Engagement.

INPUT BASED: The Consultant shall submit invoices, along with a timesheet detailing days worked and a record of any reasonable expenses, at the end of each calendar month, or upon any other interval to be agreed with the Project Director. The Consultant shall comply with such other requirements for submitting invoices as CIR may reasonably require for the purposes of complying with any client requirements. CIR will aim to pay the Consultant within 10 working days, and at the latest within 30 days, of the date of submission of such a valid and undisputed invoice.

In the event that invoices are not properly submitted, CIR reserves the right to withhold payment of the invoice. It is the Consultant's responsibility to ensure that all invoices are submitted in a timely manner. Failure to submit an invoice within 3 months following completion of the Services could result in payment being refused by CIR.

TAX

The nature of the relationship between the parties means that the Consultant is responsible for accounting for and making payment to the relevant authorities for any income tax, value added tax (if applicable), national insurance contributions/social security payments, and other such taxes required to be paid within the jurisdiction(s) relevant to the Consultant and this Agreement.

In circumstances where the relevant tax authority deems that income tax and/or other payments need to be paid by CIR on behalf of the Consultant, the Consultant undertakes to indemnify CIR against all costs, expenses and any penalty, fine or interest incurred or payable by CIR in connection with payments made by CIR to the Consultant for his/her performance of the Services detailed in this contract .CIR has the right to withhold any payments due to the consultant, if CIR have become aware of any liabilities for costs, expenses, or any penalty, fine or interest incurred by CIR in connection with or as a consequence of a claim against the consultant directly related to this contract or any previous or subsequent contract between the Consultant and CIR.

The Consultant acknowledges and agrees that they have no entitlement and do not qualify to participate in or receive any employee benefits that CIR extends to its employees.

The relationship between CIR and the Consultant is that of an Independent Consultant, therefore CIR and the Consultant both acknowledge and agree there is no agency, partnership or joint venture between them.

INSURANCE AND LIABILITY

The Consultant shall have Professional Indemnity liability cover, taken out with a reputable provider of such cover and/or shall indemnify CIR for any loss, liability, costs (including reasonable legal costs), damages or expenses arising from any breach by the consultant (or the substitute) of the terms of this Agreement. For the avoidance of

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

doubt, this includes any negligent or reckless act, omission or default in the provision of the Services. If requested to do so by CIR, the Consultant must produce a valid document of professional indemnity liability insurance and CIR may specify the amount of liability coverage required under this contract.

In the event the Consultant is providing any part of the Services outside their country of residence, the Consultant shall provide details of their emergency medical insurance coverage by email to the Project Director and any updates to those details as applicable during the provision of the Services.

In the event that CIR is required to incur medical costs on behalf of the Consultant due to the Consultant's medical and/or travel insurance not providing adequate cover, he/she undertakes to reimburse CIR for all associated costs.

- The Consultant shall be responsible for conducting an assessment of the risks to their own health and safety associated with the performance of the Services. The Consultant takes full responsibility for the risk assessment and the risks he/she bears, as well as any liabilities arising. CIR hereby disclaims all responsibilities and liabilities whatsoever and howsoever arising, to the fullest extent permitted by law.

EQUIPMENT

•

The Consultant will take due care of any CIR equipment that is used by the Consultant during the course of the assignment. The equipment provided remains the property of CIR at all times.

The Consultant shall, unless otherwise agreed with CIR, provide a laptop / PC computer with Microsoft Office and ensure this is equipped with up to date anti-virus software (ensuring virus definitions are always up to date), disk encryption and, if strictly necessary for the purpose of providing the Services, an encrypted memory stick for his or her own use during the Services. The Consultant will take particular care to ensure that no viruses are passed to other persons working on the project or to CIR or to the Client. The Consultant should avoid, whenever possible, the use of public access internet use.

In the event that Consultant uses a mobile telephone for transmitting, storing, accessing or manipulating Project Materials (defined at clause 8.3 below), such device shall be encrypted to ensure security of the data on the mobile device and equipped with up to date anti-virus software.

CONFIDENTIALITY

The Consultant hereby undertakes with CIR that the Consultant will observe the strictest conditions of confidentiality in performing the Services, and shall not divulge or use for purposes other than performing the Services, any material or information (a) relating to the business or affairs of CIR or any staff member or contractor of CIR or any Client of CIR and (b) acquired in the course of performing the Services for the Duration and this undertaking shall survive termination of this Agreement.

In order to ensure that all necessary confidentiality restrictions are complied with, and for the purpose of quality control and consistency in presentation, the Consultant is not permitted to submit to the Client any official documentation including but not limited to reports and project outputs without the prior approval of the Project Director.

The Consultant shall not, except with the prior consent of CIR or as required by law, disclose to any person, firm or company the terms of this Agreement.

Unless otherwise agreed in advance with the Project Director, the Consultant is not permitted to publish any books

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

or articles, contact the media, give any broadcasts, speeches or lectures, appear on television programmes or participate in outside conferences where such activity relates to the work of CIR and/or the Services and/or information about the Client as relates to the work of CIR or delivery of the Services.

In circumstances where the contract is funded by the UK Government the Consultant should be aware that the Official Secrets Acts 1911 to 1989 may apply to him/her. It is the Consultant's responsibility to ensure they are familiar with and act in accordance with the Act's provisions.

INTELLECTUAL PROPERTY RIGHTS AND RETURN OF MATERIALS

All intellectual property rights in all material (including but not limited to reports, data, and designs whether or not electronically stored) produced by the Consultant in the course of performing of the Services (the "Material") shall be the property of CIR. The Consultant hereby irrevocably assigns to CIR all existing and future intellectual property rights in the Material and all materials embodying these rights to the fullest extent permitted by law together with all accrued rights of action in respect of infringement of such rights. Insofar as they do not vest automatically by operation of law or under this Agreement, the Consultant holds legal title in these rights and inventions on trust for the sole benefit of CIR and shall not transfer them to a third party or encumber them.

To the extent that the Consultant has any rights, including "author's rights", "moral rights" and rights of a similar nature under the laws of any jurisdiction in respect of the Materials and/or all materials embodying such rights that cannot be assigned, the Consultant agrees unconditionally, absolutely, irrevocably, perpetually and in perpetuity to waive enforcement worldwide of such rights against CIR.

The Consultant undertakes to CIR that:

He/she has not given and will not give permission to any third party to use any of the Material nor any of the intellectual property rights in the Material;

He/she is unaware of any use by any third party of any of the Material or intellectual property rights in the Material;

The use of the Material or the intellectual property rights in the Material by CIR will not infringe the rights of any third party;

To keep confidential all Materials and details of their invention whenever requested to do so by CIR and in any event on the termination of this Agreement, promptly to deliver to CIR all correspondence, documents, papers and records on all media (and all copies or abstracts of them) recording or relating to any part of the Materials which are in his/er possession, custody or control;

not to register nor attempt to register any intellectual property rights;

to execute all documents, make all applications, give all assistance and do all acts and things, at the request and expense of CIR at any time during or after the term of this Agreement, as may, in the opinion of CIR, be necessary or desirable to vest any intellectual property rights or register them in the name of CIR and to defend CIR against any claim that any Materials infringes third party rights and otherwise to protect, maintain and enforce the intellectual property rights relating to the Materials, and to permit CIR to represent them in any matter to which there is a claim or other matter to which CIR has an interest and is directly associated with this contract .

For the avoidance of doubt, CIR shall not take ownership of any Consultant background intellectual property that was created by the Consultant independently of the Services ("Consultant Background IP"). To the extent that any Consultant Background IP becomes embedded in any of the Materials, the Consultant hereby grants to CIR, its

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

affiliates and its Client a world-wide, non-exclusive, irrevocable, royalty-free licence to use the relevant Consultant Background IP for purposes relating directly or indirectly to the objectives set out in the Terms of Reference.

The Consultant agrees to indemnify CIR and keep it indemnified at all times against all or any costs, claims, damages or expenses, including reasonable legal and accounting fees, incurred by CIR, or for which CIR may become liable, with respect to any intellectual property infringement claim or other claim relating to the Material supplied by the Consultant to CIR during the course of providing the Services.

All documents, manuals, hardware and software provided for the Consultant's use by CIR and any data or documents (including copies) produced, maintained or stored on CIR computer systems or other electronic equipment, including equipment owned by the Consultant, remain the property of CIR.

The Consultant acknowledges that no further remuneration or compensation other than that provided for in this Agreement is or may become due to the Consultant in respect of the performance of his or her obligations under this clause 7.

The provisions of this clause 7 shall survive termination of this Agreement howsoever caused..

DATA PROTECTION & DATA SECURITY

The Consultant consents to CIR and its duly authorised agents and employees holding and processing data as both data controller and data processor, both electronically and manually relating to him/her for legal, personnel, administrative and management purposes and in particular to the processing of any "sensitive personal data" and any "special category data," (as defined in the General Data Protection Regulation) relating to the Consultant including, as appropriate:

information about the Consultant's physical or mental health or condition in order to monitor sick leave and take decisions as to the Consultant's fitness for work;

the Consultant's racial or ethnic origin or religious or similar beliefs in order to monitor compliance with equal opportunities legislation; and

information relating to any criminal proceedings in which the Consultant has been involved for screening and insurance purposes and in order to comply with legal requirements and obligations to third parties.

In connection with any of the purposes described herein or any other legitimate processing of personal data, information may be shared with the overseas offices of CIR and/or independent contractors both inside and outside the EEA, subject to such overseas offices/entities being bound by the same data protection standards as the CIR's registered office in the United Kingdom and provided also that such transfer of information is necessary for the relevant purpose. CIR may subsequently use this data to comply with relevant laws such as taxation, the performance of this Agreement and/or any contract with the Client. The Consultant consents to CIR doing so as may be necessary from time to time.

The Consultant shall comply with (and not cause CIR or Client to breach) any applicable data protection legislation in any relevant jurisdiction (including the General Data Protection Regulation). If the Consultant processes any personal data on CIR's (or Client's) behalf the Consultant must (i) process the personal data in accordance with CIR's (or Client's) instructions and (ii) take all appropriate technical and organisational security measures to protect the personal data against any unauthorised or unlawful processing and any accidental loss or destruction of, or damage to, the personal data.

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

The Consultant shall at all times act with due care and skill to minimise the risk of unauthorised access or damage to, loss, unauthorised disclosure or unauthorised use of the data, software or systems of CIR or the data, software or systems of Client ("Project Materials"). The Consultant shall comply with all IT and data security policies of CIR and any Client data security policy as applicable. In the event of a data breach or suspected data breach relating to the Project Materials, the Consultant shall notify the Project Director as soon as possible and no later than 24 hours of becoming aware of the actual or potential data breach.

The Consultant shall make regular (at a minimum weekly) and secure back-ups of any Project Materials and such back-ups should be saved on the relevant CIR portal or server as applicable upon completion of the project, as set out in CIR's Backup Policy. Upon completion of the project, the Consultant should delete all Project Materials from his or her own laptop, mobile phone and any other electronic device and all hard copies of Project Materials shall be submitted to CIR or immediately destroyed, as per CIR's request.

PROTECTION OF INTERESTS

This Agreement is not intended to and shall not render the Consultant an employee, agent, or partner of CIR and for the duration of this Agreement, the Consultant shall not undertake or offer any contractual services on behalf of CIR with any third party.

The Consultant acknowledges and understands that the avoidance of a conflict of interest with CIR must be avoided at all times. Therefore, the Consultant is required to declare in writing to the Project Director any conflict, or perceived potential conflict of interest, as defined in CIR's Conflict of Interest Policy, at the earliest opportunity.

In circumstances where the Project Director reasonably considers there to be a conflict of interest that cannot be resolved through the implementation of ethical walls, the Consultant accepts and understands that he/she will be prevented from taking on the assignment or project which has given rise to the potential conflict of interest until completion of the Services.

- RESTRICTIVE COVENANTS
  - The Consultant acknowledges that in the course of providing the Services the Consultant may obtain information or develop special relationships that could place the Consultant in a position to compete unfairly with CIR. The Consultant therefore undertakes to CIR that during the term of this Agreement and for a period of 6 months following its expiration or earlier termination (howsoever arising), the Consultant will not either on the Consultant's own account or for any other person, firm or company, without obtaining the prior written consent of CIR:-
    - Solicit or canvas in competition with CIR any person, firm or company, including but not restricted to the Client, whose work requirements the Consultant has become aware of or obtained information about directly as a result of provision of the Services;
    - Solicit or endeavour to entice away from CIR any person who was employed or contracted by CIR at any time whilst the Consultant was engaged under this Agreement.
  - The Consultant shall at all times immediately refer any and all potential project or assignment enquiries relating to the Services which are raised with him/her from the Client or those associated with the Client to CIR and will not enter into competition with CIR for such work.
  - Each of the restrictions in this clause 10 are intended to be separate and severable. If any of the

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

restrictions shall be held to be void but would be valid if part of their wording were deleted or amended, such restriction shall apply with such deletion and/or amendments as may be necessary to make it valid or effective. The Consultant acknowledges and agrees expressly to the terms contained in this clause 10 and confirms that they do not restrict the Consultants ability to obtain other work in the course of his/her business.

- COMPLIANCE WITH WORKING POLICIES

  - The Consultant warrants and represents that it will observe the highest ethical standards during the performance of the Services and will comply with and apply business practices that are in compliance with the CIR Code of Conduct.
  - The Consultant will apply zero tolerance to: terrorism or the financing of terrorism; bribery or corruption of any kind; human trafficking or modern slavery; safeguarding and child protection, money laundering, fraud or tax evasion; and discrimination. The Consultant agrees to use reasonable endeavours to give effect to any reasonable request from CIR to adjust working practices for this purpose or otherwise to promote positive social or environmental impact.

- TERMINATION

  - Subject to clause 12.2 below, either party may terminate this Agreement prior to expiry of the Duration by giving to the other party not less than 14 working days written notice. For the avoidance of doubt, no notice is required to be provided to confirm completion of the Duration.
  - The Consultant will only be entitled to be paid for those days it actually worked during the 14 working day notice period and for which there was an unrescinded agreement from CIR that the Consultant would work.
  - Notwithstanding the provisions of clause 12.1 above, CIR may terminate this Agreement with immediate effect and with no liability to make any further payment to the Consultant (other than in respect of amounts accrued before the Termination Date) if at any time the Consultant:
    - commits any gross misconduct affecting the business of CIR and/or the Client;
    - commits any serious or repeated breach or non-observance of any of the provisions of this Agreement or refuses or neglects to comply

    with any reasonable and lawful directions of CIR and/or the Client;
    - is convicted of any criminal offence (other than an offence under any road traffic legislation for which a fine or non-custodial penalty is imposed);
    - is incapacitated (including by reason of illness or accident) from providing the Services for an aggregate period of 30 days in any 52 week consecutive period;
    - is certified by a duly qualified medical practitioner that he/she is incapable by reason of any accident or infirmity of mind or body of rendering further efficient and/or proper service in his/her duties;
    - commits any fraud or dishonesty or acts in any manner which in the opinion of the Executive Team of CIR brings or is likely to bring the Consultant or CIR and/or the Client into

disrepute;

- commits any act of unprofessional conduct, discrimination, harassment (sexual or otherwise) against an employee, contractor, officer or any other representative or contact of CIR or the Client;
- commits any offence under the Bribery Act 2010 and/or gives or offers to give anything of value to a foreign government employee, officer and/or agent, or carries out any other such act or omission which could, in the reasonable belief of CIR, constitute an offence under the Bribery Act 2010 or the Consultant accepts anything of value from a foreign government employee, officer and/or agent in circumstances which, in the reasonable belief of the Company, would place that foreign government, their employee, officer and/or agent in breach of the Bribery Act 2010 or any applicable local laws.
- commits any act that is determined to be a breach of security or in violation of the security rules set forth by either CIR or any security company contracted to CIR. For the avoidance of doubt, it is the responsibility of the Consultant to keep informed as to changes or updates in the security rules;
- fails to use equipment for provision of the Services that meets the standards stipulated by CIR as set out in clause 5.2 herein;
- fails any CIR and/or Client background screening processes;
- if the Client so requests;
- is in material breach of this contract.

- The rights of CIR under clause 12.2 are without prejudice to any other rights that it might have at law to terminate this Agreement or to accept any breach of this Agreement on the part of the Consultant as having brought the Agreement to an end. Any delay by CIR in exercising its rights to terminate shall not constitute a waiver of these rights.

- HEALTH
  - It is the Consultant's responsibility to ensure they are fit to travel and work and should not take risks that will impact on themselves or the project.
  - The Consultant should notify CIR prior to deployment of any medical conditions that may affect their ability to work effectively.
  - For projects that require medical clearance, Consultants must ensure that such clearance is done through an agency that specialises in face-to face medical evaluations for people deployed to hostile environments and not simply through a regular GP (unless arranged through a specialist agency).

- SOCIAL MEDIA
  - The Consultant is at all times required to adhere to CIR's policies and practices in relation to the use of social media as set out in CIR's Code of Conduct.

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

- SURVIVAL
    - The expiration or termination of the Agreement shall not affect any of those provisions which are intended and expressed to apply post termination.

- NOTICE
    - Notices by any party shall be given in writing and may be delivered personally or sent by letter (either by post or by e-mail) addressed to (in the case of CIR) its UK registered office and (in the case of the Consultant) the Consultant's last known address. Any such notice given by letter shall be deemed to have been given at the time at which the letter would be delivered in the ordinary course of post if sent by post and on the date of delivery if transmitted by e-mail.

- DISPUTE RESOLUTION
    - If a dispute arises in relation to or in connection with this Agreement, including any question regarding its existence, validity or termination, the parties will attempt to resolve it by mediation in accordance with the LCIA Mediation Rules before commencing legal proceedings.
    - If the parties fail to resolve any dispute arising out of or in connection with this Agreement through mediation in a period of thirty (30) days from the date that the mediation is initiated, the dispute shall be referred to and finally resolved through arbitration by a sole arbitrator under the Rules of the LCIA, which Rules are deemed to be incorporated by reference into this clause. The seat of the arbitration shall be London.
    - This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with English law exclusively.

- MISCELLANEOUS
    - No variation or agreed termination of this Agreement shall be effective unless it is in writing and signed by the parties (or their authorised representatives).
    - The Consultant acknowledges that in circumstances where the contract is funded by the UK Government, CIR may be required to comply with the Freedom of Information Act 2000 ("FOIA") and the Consultant agrees to comply with any reasonable instructions of CIR to enable CIR to co-operate with the UK Government on any application under FOIA.
    - The failure by a party to enforce at any time or for any period any one or more of the terms or conditions of this Agreement shall not constitute a waiver of them or of the right at any time subsequently to enforce all terms and conditions of this Agreement.
    - This Agreement and any documents referred to therein constitute the whole agreement between the parties and supersedes all previous discussions, correspondence, negotiations, arrangements, understandings and agreements between them.

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

- Each party acknowledges that, in entering into this Agreement, it has not relied on, and shall have no right or remedy (other than for breach of contract) in respect of, any statement, representation, assurance or warranty (whether made negligently or innocently) other than as expressly set out in this Agreement. Nothing in this clause shall limit or exclude any liability for fraud.
- The validity, construction and performance of this Agreement (and any claim, dispute or matter arising under or in connection with it or its enforceability) and any non-contractual obligations arising out of or in connection with it shall be governed by and construed in accordance with the law of England and Wales exclusively.
- This Agreement may be executed in any number of counterparts and by the parties to it on separate counterparts, each of which will be an original but all of which together will constitute one and the same instrument.
- This Agreement has been executed and delivered by or on behalf of the parties on the latest date of signature.

Annex 3: Statement of Compliance

I confirm that I have read, understood and accept responsibility for complying with CIR's standards of professionalism, effectiveness, integrity and ethics as set out in the following policy documents:

- Code of Conduct
- Equality Policy
- Safeguarding Policy
- Fraud, Bribery and Anti-Corruption Policy
- Data Protection, GDPR and Information Security
- Whistleblowing Policy

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

As well as the relevant sections of CIR's Finance and HR Handbook in relation to:

- Expenses
- Bullying and Harassment
- Conflict of Interest

[SIGNATURE] 
[NAME] Nina Jankowicz
[DATE] 29/09/2022

Annex 4: Declaration of Interest Form

This form should describe the nature of applicable outside interests and to the extent applicable how it creates (or could create) a conflict of interest, or perception of a conflict of interest between the interests of CIR on the one hand, and personal, professional and business interests of the Consultant on the other.

Category	Please give details of the interest and whether it applies to yourself or, where appropriate, a member of your immediate family, connected persons or some other close personal connection
Current employment and any previous employment in which you continue to have a financial interest	n/a
Appointments (voluntary or otherwise) e.g. trusteeships, directorships, local authority membership, tribunals etc	n/a

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

Membership of any professional bodies			
Investments in unlisted companies, partnerships and other forms of business, major shareholdings	n/a		
Any other conflicts that are not covered by the above	n/a		
Any current or previous Crown employment within the last two years	Please provide proof of compliance with HMG Business Appointment Rules if required n/a		
Please list any other assignments that you will be working on whilst contracted with CIR	**Names of Assignment**	**Client**	**Dates**
	Own speaking/writing engagements, eg book promotion		

I, the Consultant, hereby certify that the information above is true and complete to the best of my knowledge. In the event of any material change on new interests I will update the form as appropriate and notify the Project Director

NAME: Nina Jankowicz SIGNED: DATE: 29/09/2022

I, the Project Director or nominated substitute, have reviewed the Conflicts of Interest recorded above. The following mitigating actions have been agreed in writing with The Registrant as follows:

I hereby certify that the information above is true and complete to the best of my knowledge

NAME: Ross Burley SIGNED: DATE: 29/09/2022

Received by NSD/FARA Registration Unit 11/18/2022 12:02:17 PM

(EXHIBIT I)

Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More

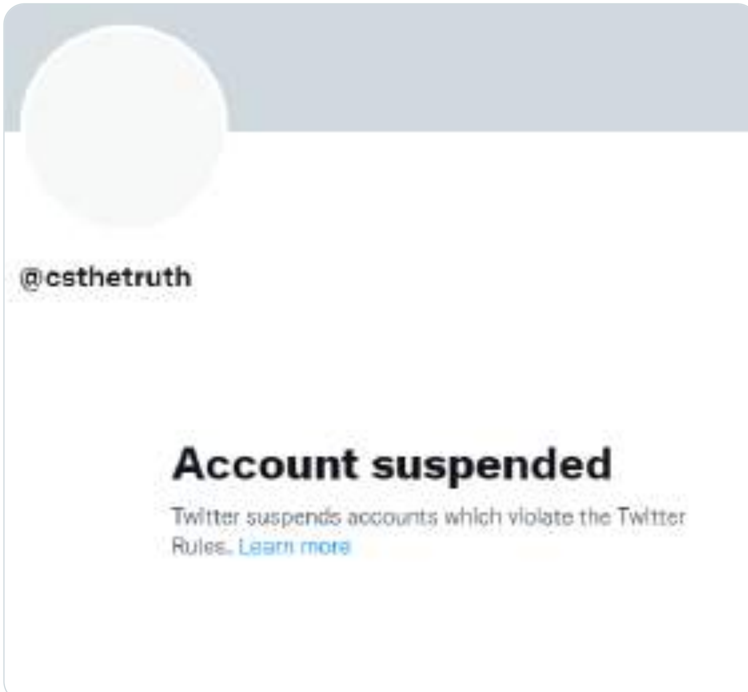
Tweet

ChrisBouzyIsGoin...
@ChrisBouzy4Jail

Tweet

Christopher Bouzy
@cbouzy

In other news, Jason Goodman's main Twitter account was suspended.



11:54 AM · Mar 18, 2022 · Twitter Web App

42 Retweets **558** Likes

Tweet your reply
Reply

Natalie Eilatan 33o1 @natalie905 · Mar 18
Replying to @cbouzy
Lol

> **Christopher Bouzy** @cbouzy · Feb 22
> The funny thing about this is that Yankee Wally and other single-purpose hate accounts thought csthetruth would be the one who brought Bot Sentinel down. Nope...😂
> Show this thread

11

DotDotDot @_Quittny · Mar 19
Replying to @cbouzy
But you'll keep us updated on him, right? Not the end of his journey.

1 3

Christopher Bouzy @cbouzy · Mar 19

Search Twitter

Relevant people

Christopher Bouzy
@cbouzy
When I was 9, I started co
Mattel Aquarius compute
developed several produc
& 30s, and then in 2018 I
BotSentinel.com

What's happening

War in Ukraine · LIVE
Ten million people have fled thei homes in Ukraine, according to the UN Refugee Agency

Politics · Trending
#HunterBidensLaptop
Trending with #BidenCrimeFamilly

Trending in Manhattan
Elon
43.8K Tweets

Sunday Times C... · This mornin
Anne Tyler: 'It would be foolish but I should be allowed to write from the viewpoint of a black man'

POPSUGAR · March 18, 2022
In Monumental News, the House of Representatives Passes the CROWN Act

Show more

Terms of Service Privacy Policy Cook
Accessibility Ads info More ···
© 2022 Twitter, Inc.

(EXHIBIT J)

Options

Thanks for your appeal

You appealed:

- 1 Tweet

CrowdsourcetheTruth
@csthetruth

#DisinfoDiva @wiczipedia is getting paid $25 grand to talk to you about #disinformation https://t.co/0r6jjdnyPN #PoorValue https://t.co/tEWRQttd9N

Jan 4, 2023, 5:48 PM

Please note that while we review your appeal, you won't be able to access your Twitter account. We'll take a look and will respond as soon as possible.

If you'd rather just delete the content, you can cancel your appeal.